UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Matjaž Košak

Sistem za podporo odločanju pri nadzoru kibernetskega tveganja v bankah

MAGISTRSKO DELO

Mentor: doc. dr. Rok Rupnik

Somentor: izr. prof. dr. Drago Bokal

Ljubljana, 2016

Številka: 153-MAG-RI/2016
Datum: 29. 02. 2016

Matjaž KOŠAK, univ. dipl. mat.

L j u b l j a n a

Fakulteta za računalništvo in informatiko Univerze v Ljubljani izdaja naslednjo magistrsko nalogo

Naslov naloge: **Sistem za podporo odločanju pri nadzoru kibernetskega tveganja v bankah**

Decision support systems for cyber-risk supervision in banks

Tematika naloge:

Tema naloge je raziskati uporabo sistemov za podporo odločanju pri identifikaciji, merjenju, upravljanju in nadzorovanju kibernetskega tveganja v bankah. Kibernetsko tveganje se z razvojem informacijske tehnologije, povezljivosti ključnih infrastrukturnih sistemov in njene kompleksnosti znatno povečuje. Predstavite zakonodajni okvir, ki opredeljuje področje IT tveganj v bankah. Preučite obstoječe metodologije, uporabljene prakse, modele oz. sisteme za podporo odločanju, ki se uporabljajo pri obravnavanju kibernetskih tveganj v bankah. Po preučitvi predstavite zasnovo konkretnega primera sistema za podporo odločanju pri oceni kibernetskega tveganja v bankah. Opozorite na pomanjkljivosti obstoječih metodologij, praks in sistemov za podporo odločanju na področju merjenja in nadzora nad kibernetskim tveganjem v bankah.
Magistrsko delo bo prispevalo k razumevanju potreb za podporo odločanju za področje kibernetskih tveganj, ki so mu banke izpostavljene ter k predstavitvi najnovejših pristopov pri merjenju kibernetskega tveganja.

M e n t o r :

doc. dr. Rok Rupnik

D e k a n :

prof. dr. Nikolaj Zimic

S o m e n t o r :

izr. prof. dr. Drago Bokal

ZAHVALA

Zahvaljujem se svojima staršema, da sta spodbujala mojo radovednost.

Kazalo vsebine

Kazalo slik

Kazalo tabel

Seznam uporabljenih kratic in simbolov

EBA	Evropski bančni organ (ang. European Banking Authority)
BIS	Banka za mednarodne poravnave (ang. Bank of International Settlements)
BCBS	Baselski odbor za bančni nadzor (ang. Basel Committee on Banking Supervision)
ECB	Evropska centralna banka (ang. European central bank)
EMN	Enotni mehanizem nadzora (ang. Single supervisory, SSM)
AMA	Napredni pristopi za merjenje (ang. Advanced Measurement Approaches)
ILD	Notranji podatki (ang. Internal loss data)
ED	Zunanji podatki (ang. External data)
BEICF	Dejavniki, ki odražajo poslovno okolje in notranje kontrole (ang. Business environment and internal control factors)
LDA	Pristop s statistično porazdelitvijo izgube (ang. Loss Distribution Approach)
SIST	Slovenski inštitut za standardizacijo
COBIT	Kontrolni cilji za informacijsko in sorodno tehnologijo (ang. Control Objectives for Information and Related Technologies)
ISACA	Združenje za revizijo in kontrolo informacijskih sistemov (ang. Information Systems Audit and Control Association)
NIS	Varnost omrežij in informacij (ang. Network and information security)
SIR	Slovenski inštitut za revizijo
ISO	Mednarodna organizacije za standardizacijo (ang. International Organization for Standardization)
IEC	Mednarodna elektrotehnična komisija (ang. International Electrotechnical Commission)
ENISA	Evropska agencija za varnost omrežij in informacij (ang. European Union Agency for Network and Information Security)
CERT	Skupina za odzivanje na računalniške grožnje (ang. Computer Emergency Response Team)
ITU	Mednarodna telekomunikacijska zveza (ang. International Telecommunication Union)
FFIEC	Zvezni svet za nadzor finančnih institucij (ang. Federal Financial Istitutions Examination Council)
NIST	Nacionalni inštitut za standarde in tehnologijo (ang. National Institute of Standards and Technology)
NISP	Javno-zasebna platforma za varnost omrežij in informacij (ang. Network Information Security Public-Private Platform)
CPMI	Odbor za plačila in tržne infrastrukture (ang. Committee on Payments and Market Infrastructures)
IOSCO	Mednarodno združenje nadzornikov trga vrednostnih papirjev (ang. International Organization of Securities Commissions)
IT	Informacijska tehnologija (ang. Information Technology)

Povzetek

Naslov: Sistem za podporo odločanju pri nadzoru kibernetskega tveganja v bankah

Avtor: Matjaž Košak

Kibernetsko tveganje se zaradi hitrega razvoja informacijske tehnologije, vse večje uporabe pametnih naprav, naprednega načina komunikacije, spreminjajočih se navad uporabnikov in iznajdljivosti kibernetskih kriminalcev povečuje. Dandanašnji kibernetski kriminalci so visoko motivirani profesionalci, ki so pogosto financirani s strani premožnih kriminalnih organizacij ali celo držav in imajo jasne cilje in strategijo.

Ker ima napačno delovanje kritičnih sistemov lahko pomembne posledice za celotno družbo, se v zadnjih letih v svetu pospešeno sprejemajo strategije in načrti in odvijajo aktivnosti za spopadanje s kibernetskimi grožnjami. Zaradi vloge, ki jo ima bančni sektor morajo biti banke sposobne natančno identificirati vsa tveganja, s katerimi se soočajo in jih ustrezno meriti, upravljati in nadzorovati. Vedno morajo imeti dovolj kapitala za kritje nepričakovanih izgub. Kibernetsko tveganje je kot del tveganj informacijske tehnologije v bančni regulativi umeščeno v sklop operativnega tveganja. Zgodnje odkrivanje potencialnih groženj je bistvenega pomena za varnost poslovanja in učinkovito upravljanje s tveganji.

V poplavi različnih metodologij, standardov, protivirusnih programov in pristopov, ki jih predpisujejo in predlagajo najrazličnejše javne in zasebne organizacije, se je pojavila potreba po sistematizaciji pristopov pri ocenjevanju kibernetskega tveganja. Sistem za podporo odločanju pri nadzoru kibernetskega tveganja v bankah, ki je predstavljen v magistrskem delu, je zasnovan na splošno sprejetih in trenutno veljavnih industrijskih standardih s področja informacijske varnosti in zagotavlja skupno osnovo za razumevanje, ocenjevanje in upravljanje kibernetskega tveganja. Predstavljen sistem za podporo odločanju pri nadzoru kibernetskega tveganja v bankah oceni tvegaje banke na podlagi ocene delovanja kontrolnih mehanizmov ter inherentnega tveganja. Nato identificira kritična področja ter v primeru povečanega tveganja predlaga ukrepe za zmanjšanje tveganja, kar omogoča lažje vsebinsko odločanje pri izbiri ukrepov pri nadzoru kibernetskega tveganja v bankah.

Ključne besede: Sistem za podporo odločanju, nadzor kibernetskega tveganja v bankah, kibernetska kriminaliteta, tveganje IT, kibernetske grožnje.

Abstract

Title: Decision support systems for cyber risk supervision in banks

Author: Matjaž Košak

Cyber risk has been increasing due to fast development of information technology, increased using of smart gadgets, advanced way of communication, changing habits of users, and inventiveness of cyber criminals. Nowadays, cyber criminals are highly motivated professionals who are frequently financed by wealthy criminal organizations, or even states, and have clear goals and strategies.

False working of critical systems might have important consequences for the whole society, therefore the pace of the new strategies, plans, and different activities to fight cyber threats is being stepped up in the last years around the world. Because of the bank sector role, banks have to be able to precisely identify all risks they face and measure, manage, and control them. They must have enough capital to cover unexpected loss. Cyber risk as a part of information technology risk is placed in the system of operational risk. Early uncovering of potential threats is essential for security of business and efficient managing of risks.

The abundance of new methodologies, standards, antivirus programmes and approaches that have been prescribed and proposed by different public and private organizations has brought with it a need for a systematic approach to assessing the cyber risk. The decision support system for cyber risk supervision in banks, which is presented in the master's thesis, is based on generally accepted and currently valid industrial standards pertaining to information security and provides for a general basis for understanding, assessment and management of cyber risks. The presented decisions support system for the supervision of cyber risk in banks evaluates the bank's risk based on the assessment of the inherent risk and the functioning of control mechanisms. It goes on to identify critical areas and suggests measures to mitigate the risk, which in turn enables more efficient decision-making as to the measures for the supervision of cyber risk in banks.

Keywords: Decision support systems, cyber risk supervision in banks, cybercrime, IT risk, cyber threats

1 Uvod

Kibernetska in informacijska varnost postaja ob vse večji uporabi informacijskih sistemov, njihovi vse večji povezljivosti in integriranosti v ključne infrastrukturne sisteme vse bolj pomembna za nemoteno delovanje sistemov, pomembnih za delovanje celotne družbe. Prekinitve delovanja, napačno delovanje ali zloraba podatkov in pooblastil lahko ogrozijo delovanje kritičnih sistemov, kar ima lahko za posledico ogrožanje nacionalne varnosti, zdravja prebivalstva in v najboljšem primeru poslovno škodo. Po zadnjih raziskavah se je število varnostnih incidentov v EU v letu 2015 povečalo za 38 % [27]. Ni presenetljivo, da se v zadnjih letih pospešeno sprejemajo strategije za soočanje s tovrstnimi nevarnostmi na obrambnem, obveščevalnem, finančnem in drugih področjih. Strategija kibernetske varnosti Evropske unije (ang. *Cybersecurity Strategy for the European Union*) [16] in Evropska agenda za varnost (ang. *European Agenda on Security*) [17] predstavljata strateško ogrodje EU na področju kibernetske varnosti in kriminala.

Bančni sektor je izjemnega pomena za delovanje gospodarstva. Osnovna naloga bank je hranjenje prihrankov varčevalcev, opravljanje storitev plačilnega prometa in posojanje denarja investitorjem. Predvsem zaradi hranjenja prihrankov varčevalcev in upravljanja z njihovimi prihranki so banke podvržene izredno strogim regulatornim zahtevam. Banke morajo biti sposobne natančno identificirati vsa tveganja, s katerimi se soočajo, in jih ustrezno meriti, upravljati in nadzorovati. Kibernetsko tveganje bank ni nobena izjema. Zaradi krize, v kateri se je znašel bančni sektor, so bili v zadnjem obdobju v središču pozornosti predvsem kreditno, likvidnostno in tržno tveganje, načini upravljanja bank, vzdržnost poslovnega modela in dobičkonosnost. Predvsem zaradi nižje dobičkonosnosti bank, hude konkurence med bankami in varčevanja v zadnjih letih so bila vlaganja v posodabljanje IT infrastrukture manjša, kar še dodatno postavlja pod vprašaj ustreznost obravnave kibernetskega tveganja v bankah.

Kibernetsko tveganje in kibernetska kriminaliteta se zaradi hitrega razvoja informacijske tehnologije, povečanega poslovanja preko sodobnih elektronskih poti in vse večje uporabe pametnih naprav ter iznajdljivosti kibernetskih kriminalcev neprestano spreminjata, zaradi česar je kibernetsko tveganje težje ocenjevati. Kibernetski napadi postajajo del vsakdana tako za posameznike in za podjetja kot tudi za institucije.

Banke morajo ne ozirajoč se na tveganje informacijske tehnologije imeti vzpostavljeno učinkovito in stabilno ureditev notranjega upravljanja z jasno organizacijsko strukturo in z natančno opredeljenimi odgovornostmi, imeti učinkovite procese za ugotavljanje, ocenjevanje, obvladovanje in spremljanje vseh tveganj. Prav tako morajo imeti vzpostavljene mehanizme notranjih kontrol ter izjemno učinkovit sistem na področju poročanja ter internega nadzora.

Bančno poslovanje redno pregledujejo in spremljajo zunanji revizorji, bonitetne agencije, centralne banke oziroma bančni regulatorji.

V magistrskem delu je predstavljen zakonodajni ovir in obstoječe metodologije, v okviru katerih banke upravljajo s kibernetskimi tveganji. Opisane so najnovejše kibernetske grožnje in

primeri najodmevnejših napadov na banke. Predstavljene so osrednje institucije, zakonodajna podlaga in strategije v povezavi s soočenjem s kibernetskim tveganjem tako v Sloveniji kot tudi v EU. Predstavljeni so primeri dobrih praks pri identifikaciji in merjenju kibernetskega tveganja, ki se razvijajo v zadnjem obdobju v Evropi in po svetu. Na podlagi najboljših praks je zasnovan in predstavljen sistem za podporo odločanju pri nadzoru kibernetskega tveganja v bankah. Sistem oceni kibernetsko tveganje preko ocene osnovnih elementov kibernetskega tveganja. Osnovni elementi temeljijo na splošno sprejetih in trenutno veljavnih industrijskih standardih s področja informacijske varnosti. Na podlagi ocen osnovnih elementov sistem združuje ocene osnovnih elementov v posamezne kategorije in na koncu v skupno oceno kibernetskega tveganja banke. Če je ocena tveganja visoka, sistem za podporo odločanju identificira problematična področja in predlaga ukrepe za zmanjšanje kibernetskega tveganja. Sistem za podporo odločanju pri nadzoru kibernetskega tveganja v bankah zagotavlja enotno podlago za razumevanje, ocenjevanje in nadzorovanje kibernetskega tveganja.

2 Tveganja in nadzor v bankah

Banke so pri svojem poslovanju izpostavljene različnim vrstam tveganja. Banke morajo biti sposobne tveganja identificirati, da jih lahko nato merijo, spremljajo in upravljajo.

V skladu s 147. členom Zakona o bančništvu (Ur. l. RS, št. 25/2015) mora uprava banke zagotoviti ustrezne kadrovske in finančne vire za učinkovito in celostno obravnavo tveganj v banki, vključno z ugotavljanjem, merjenjem oziroma ocenjevanjem, spremljanjem in obvladovanjem tveganj, ki jim je banka izpostavljena pri svojem poslovanju, ali ki bi jim lahko bila izpostavljena. Prav tako morata uprava in nadzorni svet nameniti dovolj časa obravnavi tveganj. Vzpostaviti morata sistem poročanja, ki zagotavlja, da sta uprava in nadzorni svet pravočasno seznanjena o vseh pomembnih tveganjih banke, in ki upošteva politiko upravljanja tveganj in njene spremembe [40].

V Sklepu o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice (Ur. l. RS, št. 73/2015 v nadaljevanju Sklep o ureditvi notranjega upravljanja) so v 19. členu navedena sledeča tveganja, ki jih banka lahko prevzema v okviru svojega poslovanja, in sicer: kreditno tveganje in tveganje nasprotne stranke, tveganje koncentracije v okviru kreditnega tveganja, tržna tveganja, obrestno tveganje, likvidnostno tveganje, operativno tveganje (vključno s pravnim tveganjem), tveganje skladnosti, modelsko tveganje, tveganje ugleda, strateško tveganje, kapitalsko tveganje, tveganje dobičkonosnosti, tveganje prevelikega finančnega vzvoda in tveganja, povezana z listinjenjem [33].

Poleg splošnih zahtev v povezavi z upravljanjem tveganj iz Sklepa mora banka dodatno izpolnjevati še zahteve glede obravnave naslednjih tveganj: kreditno tveganje, likvidnostno tveganje, operativno tveganje, tržna tveganja [33].

Kibernetsko tveganje je kot del tveganj informacijske tehnologije (ang. *Information Technology,* v nadaljevanju IT) v bančni regulativi umeščeno v sklop operativnega tveganja.

Zaradi posebne vloge v gospodarstvu in upravljanja tujega denarja (hranjenje vlog prebivalstva in gospodarstva) je banka podvržena strogim kapitalskim zahtevam. Primerna višina kapitala banke ščiti varčevalce in investitorje pred izgubo svojih prihrankov, saj v primeru nepričakovanih izgub banka le-te krije s kapitalom. Ne glede na sposobnost banke za poravnavo svojih obveznosti so do višine 100.000 EUR zajamčene skupno vse vloge, ki jih imajo fizične osebe in manjša podjetja pri posamezni banki ali hranilnici v RS, kar ureja Zakon o sistemu jamstva za vloge (Uradni list RS, št. 27/16) [44].

2.1 Baselski standardi in kapitalske zahteve

Baselski odbor za bančni nadzor (ang. *Basel Committee on Banking Supervision*, *BCBS*) je bil ustanovljen leta 1974 z namenom zagotavljanja stabilnosti v mednarodnem bančnem sistemu. Odbor je bil sestavljen iz predstavnikov držav G-10. Danes Baselski odbor za bančni nadzor sestavljajo predstavniki iz 27 držav, med drugim Argentine, Brazilije, Avstralije, Kitajske, Indije, Rusije, Savdske Arabije, Nemčije, Velike Britanije, Kanade, ZDA in Švice. Baselski odbor za bančni nadzor ima sedež v Banki za mednarodne poravnave (*Bank of International Settlements, BIS*) v Baslu v Švici.

Naloga Baselskega odbora za bančni nadzor je pripravljati priporočila, memorandume, osnutke regulacij, smernice in standarde na področju bančnega poslovanja. Standardi neposredno sicer niso zavezujoči, vendar jih države praviloma vgradijo v nacionalno zakonodajo. Na podlagi prvega kapitalskega sporazuma iz leta 1988 so bile sprejete minimalne kapitalske zahteve v več kot 100 državah. Zaradi močne podpore ključnih svetovnih držav in doseženega konsenza si zaradi mednarodnega konkurenčnega okolja nobena mednarodno vpeta država ali banka ne more privoščiti, da bi ignorirala baselska priporočila. Zaupanje v banko in v bančni sistem bi bilo v tem primeru preveč okrnjeno in bi pomenilo izolacijo. Pogosto države standarde, ki jih priporoča Baselski odbor za bančni nadzor, pri prenosu v lokalno zakonodajo še nadgradijo oziroma dopolnijo.

Najbolj znani produkti Baselskega odbora za bančni nadzor so sporazumi, ki so vzpostavili pravila glede minimalnih kapitalskih zahtev, izvajanja nadzora in tržne discipline (razkrivanje informacij, transparentnost informacij, obveščanje javnosti). Gre za sporazum »Mednarodno približevanje merjenja kapitalske ustreznosti in kapitalskih zahtev« (ang. *International convergence of capital measurement and capital standards*) iz leta 1988, poznan kot Basel I, njegova obsežnejša nadgradnja iz leta 2004, poznan kot Basel II, in sporazum iz decembra 2010, poznan kot Basel III, ki ga je spodbudila finančna kriza, ki se je začela leta 2008. Basel III postavlja višje kapitalske zahteve ter določa okvir likvidnostne regulacije in trenutno predstavlja najnovejši globalni okvir za bančni nadzor. Operativna tveganja so bila prvič opredeljena do potankosti v sporazumu Basel II.

Skupina G-20 je v izjavi z dne 2. aprila 2009 o krepitvi finančnega sistema pozvala k mednarodno usklajenemu prizadevanju za okrepitev preglednosti, odgovornosti in regulativne ureditve z izboljšanjem količine in kakovosti kapitala v bančnem sistemu, potem ko bo zagotovljena oživitev gospodarstva. V tej izjavi sta bili izraženi tudi zahtevi po i) uvedbi dodatnega ukrepa, ki ne bi temeljil na tveganju in s katerim bi se omejilo povečevanje finančnih vzvodov v bančnem sistemu ter ii) razvoju okvira za večje likvidnostne blažilnike. Septembra 2009 se je skupina guvernerjev centralnih bank in glavnih nadzornikov na podlagi mandata, ki ji ga je podelila skupina G-20, dogovorila o več ukrepih za okrepitev regulativne ureditve bančnega sektorja. Te ukrepe so na vrhu v Pittsburghu, ki je potekal 24. in 25. septembra 2009, potrdili voditelji držav G-20. Decembra 2010 je Baselski odbor za bančni nadzor objavil končne ukrepe, na katere se sklicuje kot na okvir Basel III.

Pravno je sporazum Basel III implementiran v uredbi in direktivi Evropskega parlamenta in Sveta z dne 26. junija 2013, in sicer:

- Uredba (EU) št. 575/2013 – Uredba o kapitalskih zahtevah (ang. *Capital Requirements Regulation*, uredba CRR),
- Direktiva 2013/36/EU – Direktiva o kapitalskih zahtevah IV (ang. *Capital Requirements Directive*, direktiva CRD IV),

ki sta znani kot paket CRR/CRD IV in skupaj tvorita pravni okvir za poslovanje in bančni nadzor.

Končno besedilo je bilo objavljeno v uradnem glasilu EU konec junija 2013. Nova pravila so vstopila v veljavo s 1. januarjem 2014. Sama implementacija sporazuma Basel III je postopna in bi naj bila dokončana do leta 2019.

Ključna razlika med direktivo in uredbo je v tem, da je uredba, ki jo sprejme Evropski parlament, zakonsko neposredno zavezujoča za države članice Evropske unije, medtem ko morajo države članice Evropske unije direktivo ustrezno prenesti v nacionalno zakonodajo. Slovenija je direktivo 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 prenesla v pravni red Republike Slovenije preko Zakona o bančništvu in preko Sklepa o ureditvi notranjega upravljanja.

Kapitalski sporazum Basel III sestavljajo trije stebri:

- Prvi steber določa izračun minimalnega kapitala, ki ga mora imeti banka za kritje potencialnih izgub iz kreditnega, tržnega in operativnega tveganja. Prav tako določa zahteve, ki jih mora banka upoštevati na področju likvidnosti.
- Drugi steber določa način nadzora nad bankami ter procese identificiranja vseh ostalih tveganj, ki jim je banka izpostavljena.
- Tretji steber določa način zagotavljanja tržne discipline, transparentnosti poslovanja ter obveščanje javnosti.

Za izračun potrebnega minimalnega kapitala, ki ga mora imeti banka za kritje potencialnih izgub iz naslova posameznih tveganj, lahko banka izbere različne metode.

V poglavju »3. Merjenje operativnega tveganja« so predstavljeni pristopi za izračun kapitalskih zahtev za operativna tveganja, v okviru katerih so zajeta tveganja, povezana z informacijsko tehnologijo in kibernetskimi grožnjami.

2.2 Evropski bančni organ

Eno od osrednjih vlog pri nadzoru bančnega tveganja v evropskem bančnem nadzoru ima Evropski bančni organ (ang. *European Banking Authority*, v nadaljevanju EBA), ki je neodvisen organ, odgovoren Evropskemu parlamentu, Svetu Evropske unije in Evropski komisiji. Organ EBA je bil ustanovljen z uredbo št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010. Organ EBA je agencija EU s sedežem v Londonu.

Ustanovitev organa EBA je spodbudila finančna kriza, ko so se pokazale pomanjkljivosti na področju sodelovanja in usklajevanja med bančnimi nadzornimi institucijami v državah EU. Namen ustanovitve organa EBA je zagotoviti učinkovito in usklajeno stopnjo ureditve varnega in skrbnega poslovanja ter nadzora v evropskem bančnem sektorju. Splošna cilja organa EBA sta ohranjati finančno stabilnost v EU ter zagotavljati integriteto, učinkovitost in pravilno delovanje bančnega sektorja.

Organ EBA pripravlja osnutke regulativnih in izvedbenih tehničnih standardov, ki jih potrdi Evropska komisija, in sprejema zavezujoče tehnične standarde ter priporočila in smernice. Organ EBA ima ključno vlogo pri zbliževanju nadzorniških praks med državami EU in prispeva k vzpostavitvi enotnih evropskih pravil v bančništvu, kar zadeva tudi kibernetska tveganja. Ocenjuje tudi tveganja in ranljivosti v bančnem sektorju EU, predvsem z izvajanjem rednih stresnih testov po vsej Evropi.

Poleg osnovnih nalog je organ EBA pooblaščen tudi, da ugotavlja uporabo prava EU v nacionalnih organih, sprejema odločitve v izrednih razmerah, posreduje v sporih med pristojnimi organi v EU ter svetuje Evropskemu parlamentu, Svetu EU in Evropski komisiji.
Organ EBA mora svoje naloge in pooblastila izvajati učinkovito in pregledno. O vseh tehničnih dokumentih, ki jih EBA pripravi, razpravljajo delovne skupine in stalni odbori, katerih člani so organi iz nacionalnih državi. Pri izvajanju svojih pooblastil redno sodeluje tudi z drugimi organi in institucijami. Da lahko interesne skupine in vse zainteresirane strani prispevajo svoje predloge, glede prihodnjih bančnih standardov in smernic, se po potrebi organizirajo odprta javna posvetovanja o regulativnih dokumentih [9].

2.3 Evropska centralna banka

Kljub ustanovitvi organa EBA, ki je pomembno prispeval k izboljšanju sodelovanja med bančnimi nadzornimi organi v državah EU in k enotnim pravilom za finančne storitve v EU, pa je nadzor nad bankami v veliki meri ostal v pristojnosti držav članic. Ravno pomanjkljivosti pri nadzoru pa so že v začetku bančne krize prispevale k napetostim med državami članicami. V okviru krepitve dolgoročnega zaupanja v banke in v evro je bil v okviru Evropske centralne banke (v nadaljevanju ECB) ustanovljen Enotni mehanizem nadzora (ang. *Single supervisory mechanism – SSM*, v nadaljevanju EMN), ki predstavlja popolnoma nov sistem bančnega nadzora v Evropi. Sestavljajo ga ECB in nacionalni nadzorni organi sodelujočih držav. ECB ima pooblastila, da izvaja nadzorniške preglede, inšpekcijske preglede na kraju samem in preiskave, izdaja in odvzema dovoljenja za opravljanje bančnih storitev, oceni pridobitve in odsvojitve kvalificiranih deležev, skrbi za spoštovanje bonitetnih pravil EU in določi višje kapitalske zahteve (»blažilnike«), če je to potrebno, da bi zmanjšala finančna tveganja. ECB trenutno neposredno nadzira približno 130 najpomembnejših bank v evroobmočju, kar predstavlja več kot 80 % bilančne vsote bank v evroobmočju.

Pravna podlaga za vzpostavitev EMN je Uredba Sveta (EU) št. 1024/2013 z dne 15. oktobra 2013 o prenosu posebnih nalog, ki se nanašajo na politike bonitetnega nadzora kreditnih institucij, na ECB [36], in pa Uredba (EU) št. 468/2014 ECB z dne 16. aprila 2014 o vzpostavitvi okvira za sodelovanje znotraj EMN med ECB in pristojnimi nacionalnimi organi ter z imenovanimi nacionalnimi organi (okvirna Uredba o EMN) [34].

Z vzpostavitvijo Enotnega mehanizma nadzora je ECB pričela izvajati bančni nadzor na popolnoma operativni ravni. Celotni proces od prvih idej o vzpostavitvi EMN do dejanske uveljavitve je bil zelo zahteven in je vključeval usklajevanja med različnimi državami in institucijami. EMN je sedaj pred zahtevnim obdobjem, ko je potrebno velike ideje, ki so dobile zakonsko podlago, dejansko udejanjiti v praksi. Zaradi pridobivanja na pomembnosti je kibernetsko tveganje eno tistih, ki mu je namenjeno precej pozornosti. V EMN je trenutno zaposlenih okrog 1000 posameznikov iz različnih držav EU. Prepletanje nadzorniških praks iz različnih držav, izmenjava izkušenj in tudi nacionalne lastnosti predstavljajo izziv za EMN pri uresničevanju svojega poslanstva.

3 Merjenje operativnega tveganja v bankah

Uredba o kapitalskih zahtevah (CRR) definira "operativno tveganje" kot tveganje izgube zaradi neprimernega ali neuspešnega izvajanja notranjih procesov, ravnanj ljudi in delovanja sistemov ali zaradi zunanjih dogodkov ter vključuje pravno tveganje [35].

Operativno tveganje v bančništvu je pridobilo na pomembnosti šele v zadnjem desetletju. Temu je botrovalo čedalje kompleksnejše poslovanje bank ter njihova povečana odvisnost od podpornih sistemov in vplivov človeškega faktorja. Kapitalske zahteve za operativno tveganje so bile vpeljane z drugim kapitalskim sporazumom Basel II.

Upravljanje oz. merjenje operativnega tveganja je opredeljeno z Uredbo o kapitalskih zahtevah [35], Direktivo o kapitalskih zahtevah [6], smernicami in navodili pristojnih institucij in z zakonodajnimi akti v posameznih državah.

Študija »Trendi, oblike in varnostni protiukrepi« (ang. *Trends, Patterns and Security Countermeasures*), osnovana na vzorcu več kot 15 milijonov kibernetskih napadov, predstavljena na sedmi mednarodni konferenci o finančni kriminologiji aprila 2015, je pokazala, da so bile varnostne kršitve v manj kot polovici primerov posledice načrtovanih napadov. Glavni vzroki varnostnih kršitev so poleg načrtovanih napadov še človeška napaka in ranljivost sistemov [2].

Velik izziv predstavljajo za banko primeri notranjih goljufij in zlorab, saj jih je zelo težko modelirati in vnaprej predvideti način zlorabe. Varčevanje pri posodabljanju IT opreme omogoča lažje zlorabe, obenem pa varčevanje pri nagrajevanju dodatno spodbuja zaposlene, da poskušajo z zlorabo informacij priti do osebnih koristi. Pomembno je tudi vzdušje oziroma odnos do prevar in zlorab, ki je prisotno v podjetju oziroma organizaciji. Dodaten problem pri notranjih goljufijah in zlorabah podatkov je tudi to, da se jih običajno odkrije pozno. Vsesplošna povezljivost in prisotnost informacijskih orodij in pametnih naprav (mobilne naprave, ključ USB itd.) še dodatno olajša krajo in zlorabo podatkov. Pri preprečevanju notranjih goljufij in zlorab se banke poslužujejo analiz obnašanja zaposlenih na podlagi njihovih profilov oziroma zabeleženih aktivnosti v sistemih [8].

3.1 Izračun kapitalskih zahtev za operativno tveganje

Kapitalske zahteve za operativno tveganje naj bi zagotavljale, da imajo banke dovolj kapitala za kritje nepričakovanih izgub iz naslova operativnega tveganja, vendar same po sebi neposredno ne vplivajo na izpostavljenost banke operativnemu tveganju. Pri izračunu kapitalskih zahtev bančna regulativa spodbuja banke k uporabi naprednih pristopov, ki temeljijo na modelih in zahtevajo poglobljeno upravljanje operativnih tveganj. Glede na različne poslovne modele, kompleksnost in naravo bank oziroma izpostavljenost tveganjem so na voljo različni pristopi za izračun kapitalskih zahtev za operativno tveganje.

Banke morajo javno razkriti pristope, ki jih uporabljajo za izračun kapitalskih zahtev za operativno tveganje ter opis metodologije. Banke imajo za izračun kapitalskih zahtev za operativno tveganje na voljo enostavni pristop (ang. *Basic Indicator Approach*), standardiziran pristop (ang. *Standardised Approach*) in napredni pristop (ang. *Advanced Measurement Approach*).

- **Enostavni pristop**

V skladu z enostavnim pristopom je kapitalska zahteva za operativno tveganje enaka 15 % triletnega povprečja relevantnega kazalnika. Relevantni kazalnik je dohodkovni kazalnik in vsebinsko ustreza bruto dohodku banke. Kapitalska zahteva za operativno tveganje tako ustreza 15 % bruto dohodka banke, ne glede na dejansko izpostavljenost banke operativnemu tveganju. Enostaven pristop je zelo omejen in primeren za banke z omejenim obsegom poslovanja.

- **Standardiziran pristop**

Standardiziran pristop in alternativni standardizirani pristop sta podobna enostavnemu pristopu s to razliko, da banka nekoliko drugače uteži (od 12 % do 18 %) relevantni kazalnik za posamezna poslovna področja.

Enostavni in (alternativni) standardiziran pristop ne zahtevata od banke izpolnjevanja zahtevnih standardov merjenja operativnega tveganja, sta pa zato običajno precej bolj konservativna oziroma potratna glede kapitala, ki ga mora imeti banka za kritje nepričakovanih izgub. Ker so stroški kapitala visoki, banke stremijo k uporabi naprednih pristopov, ki precej bolj natančno določajo potrebni kapital, ki ga mora imeti banka na razpolago za kritje nepričakovanih izgub.

- **Napredni pristop**

Banke lahko uporabljajo napredne pristope za merjenje operativnega tveganja (ang. *Advanced Measurement Approaches, AMA*), ki temeljijo na njihovih lastnih sistemih za merjenje, če poleg splošnih standardov upravljanja izpolnjujejo tudi dodatne zahtevne kvalitativne in kvantitativne zahteve in dobijo dovoljenje nadzornih organov.

3.2 Zahteve pri uporabi naprednih pristopov za izračun kapitalskih zahtev

Kvalitativni standardi, ki jih določa Uredba o kapitalskih zahtevah pri uporabi naprednih pristopov, so [35]:

a) Sistem institucije za notranje merjenje operativnega tveganja je tesno vključen v njene vsakodnevne procese upravljanja tveganj.
b) Institucija ima neodvisno funkcijo za upravljanje operativnega tveganja.
c) Institucija ima sistem za redno poročanje o izpostavljenostih operativnemu tveganju in o preteklih izgubah ter imajo postopke za sprejemanje ustreznih popravnih ukrepov.
d) Sistem institucije za upravljanje tveganj je dobro dokumentiran. Institucija ima vzpostavljene redne postopke za zagotavljanje skladnosti in politike za obravnavo neskladnosti.
e) Postopke institucije za upravljanje operativnega tveganja in njene sisteme merjenja operativnega tveganja redno pregledujejo notranji ali zunanji revizorji.
f) Notranji postopki institucije za ovrednotenje institucije so zanesljivi in učinkoviti.
g) Podatkovni tokovi in procesi, ki so povezani s sistemom institucije za merjenje tveganj, so pregledni in dostopni.

Kvantitativni standardi, ki jih določa Uredba o kapitalskih zahtevah pri uporabi naprednih pristopov, v povezavi s procesom so [35]:

a) Institucija izračuna svojo kapitalsko zahtevo z vključitvijo tako pričakovane izgube kakor tudi nepričakovane izgube, razen če je pričakovana izguba ustrezno zajeta v njihovih notranjih poslovnih praksah. Mera operativnega tveganja zajame potencialno resne dogodke z dna spodnjega dela statistične porazdelitve izgub, pri čemer mora doseči standard zanesljivosti, primerljiv z 99,9 % intervalom zaupanja v obdobju enega leta.
b) Sistem institucije za merjenje operativnega tveganja vključuje uporabo notranjih podatkov, zunanjih podatkov, analiz scenarijev in dejavnikov, ki odražajo poslovno okolje ter sisteme notranjih kontrol. Institucija ima vzpostavljen dobro dokumentiran pristop za tehtanje uporabe teh štirih elementov v svojem sistemu za merjenje celotnega operativnega tveganja.
c) Sistem institucije za merjenje tveganja zajema glavne dejavnike tveganja, ki vplivajo na obliko spodnjega dela ocenjene statistične porazdelitve izgub.
d) Institucija lahko prepozna korelacije pri izgubah zaradi operativnega tveganja po posameznih ocenah operativnega tveganja samo, če so njeni sistemi merjenja korelacij zanesljivi, se izvajajo celovito in upoštevajo negotovost, ki se pojavlja pri vseh takih ocenah korelacij, zlasti v stresnih obdobjih. Institucija ovrednoti svoje predpostavke o korelacijah z uporabo ustreznih kvantitativnih in kvalitativnih tehnik.

e) Sistem institucije za merjenje tveganja je notranje dosleden in se izogiba večkratnemu štetju kvalitativnih ocen ali tehnikam zmanjševanja tveganja, priznanih v drugih delih te uredbe.

Kvantitativni standardi, ki jih določa Uredba o kapitalskih zahtevah pri uporabi naprednih pristopov, v povezavi z notranjimi podatki so [35]:

a) Institucija kot podlago za svoje notranje generiranje mer operativnega tveganja uporabi najmanj petletno preteklo obdobje opazovanja. Ko institucija prvič preide na pristop AMA, lahko uporabi triletno preteklo obdobje opazovanja.
b) Institucija je sposobna razporediti svoje pretekle notranje podatke o izgubi po poslovnih področjih in po vrstah dogodkov ter te podatke na zahtevo zagotovi pristojnim organom. V izjemnih okoliščinah lahko institucija škodne dogodke, ki vplivajo na celotno institucijo, razporedi v dodatno poslovno področje "korporativne postavke". Institucija ima dokumentirana, objektivna merila za razporejanje izgub po določenih poslovnih področjih in vrstah dogodkov. Institucija evidentira izgube iz naslova operativnega tveganja, ki so povezane s kreditnim tveganjem in so bile v instituciji v preteklosti vključene v notranje baze podatkov o kreditnem tveganju, v baze podatkov o operativnem tveganju in jih ločeno označi. Takšne izgube niso predmet kapitalske zahteve za operativno tveganje, dokler jih morajo institucije pri izračunu zahtev po lastnih sredstvih še naprej obravnavati kot kreditno tveganje. Institucija vključi izgube iz naslova operativnega tveganja, ki so povezane s tržnimi tveganji, v okvir kapitalske zahteve za operativno tveganje.
c) Notranji podatki o izgubi institucije so celoviti v smislu, da zajemajo vse pomembne dejavnosti in izpostavljenosti iz vseh ustreznih podsistemov ter geografskih lokacij. Institucija je sposobna utemeljiti, da katere koli izključene dejavnosti ali izpostavljenosti, tako posamezno kot v kombinaciji, nimajo pomembnega vpliva na ocene celotnega tveganja. Institucija opredeli ustrezne spodnje prage izgub za namen zbiranja notranjih podatkov o izgubi.
d) Poleg informacij o bruto zneskih izgube institucija zbira informacije o datumu škodnega dogodka, morebitnih povračilih od bruto zneskov izgube, prav tako pa tudi opisne informacije o dejavnikih ali vzrokih škodnega dogodka.
e) Institucija ima posebna merila za razporejanje podatkov o izgubi, ki izhajajo iz škodnega dogodka v centralizirani dejavnosti ali dejavnosti, ki se razteza čez več kot eno poslovno področje, kakor tudi iz povezanih škodnih dogodkov skozi čas.
f) Institucija ima dokumentirane postopke za ocenjevanje stalne relevantnosti podatkov o pretekli izgubi, vključno z okoliščinami, v katerih se lahko podatki spremenijo zaradi strokovne ocene ter uporabijo prilagoditvena merila ali druge prilagoditve, ter v kakšni meri se lahko uporabijo in kdo je pooblaščen za sprejemanje takih odločitev.

Kvantitativni standardi, ki jih določa Uredba o kapitalskih zahtevah pri uporabi naprednih pristopov, v povezavi z zunanjimi podatki so [35]:

a) Sistem institucije za merjenje operativnega tveganja uporablja ustrezne zunanje podatke, zlasti če je utemeljeno pričakovati, da je institucija izpostavljena sicer redkim, vendar potencialno hudim izgubam. Institucija ima sistematičen proces za določanje razmer, v katerih se uporabijo zunanji podatki, in metodologije za vključitev podatkov v svoj sistem merjenja.
b) Institucija redno pregleduje pogoje in prakse v povezavi z uporabo zunanjih podatkov ter jih dokumentira in da v reden neodvisni pregled.

Kvalifikacijski standardi, ki jih določa Uredba o kapitalskih zahtevah pri uporabi naprednih pristopov, v povezavi z dejavniki poslovnega okolja in notranjih kontrol so [35]:

a) Metodologija institucije za merjenje tveganja na najvišji ravni zajame ključne dejavnike poslovnega okolja in notranjih kontrol, ki lahko spremenijo njen profil operativne tveganosti.
b) Institucija upraviči izbiro vsakega dejavnika kot pomembnega nosilca tveganja na podlagi izkušenj in vključitve strokovne ocene vključenih poslovnih področij.
c) Institucija je pristojnim organom sposobna utemeljiti občutljivost ocen tveganja na spremembe dejavnikov in relativno utež različnih dejavnikov. Poleg zajemanja sprememb tveganja zaradi izboljšav nadzorovanja tveganja okvir institucije za merjenje tveganja zajame tudi potencialna povečanja tveganja zaradi večje zapletenosti dejavnosti ali povečanega obsega poslovanja.
d) Institucija dokumentira svoj okvir za merjenje tveganja ter ga podvrže neodvisnemu pregledu znotraj institucije in s strani pristojnih organov. Po določenem obdobju institucija ovrednoti proces in njegove rezultate ter oboje ponovno oceni na podlagi primerjave z dejansko notranjo izgubo in relevantnimi zunanjimi podatki.

3.3 Škodni dogodki in podatkovni podatki

Če želi banka uporabljati napredne pristope za merjenje in izračun kapitalske zahteve za operativno tveganje, mora vzpostaviti celovit sistem identificiranja beleženja, spremljanja in analiziranja podatkov o vseh preteklih škodnih dogodkih in potencialnih škodnih dogodkih.

Kategorije, v katere mora banka razvrščati škodne dogodke, pri uporabi naprednih pristopov, so [35]:

- Notranja goljufija

  Izgube zaradi vrste dejanj, katerih namen je poneverba, odtujitev lastnine ali izogibanje predpisom, zakonodaji ali politiki podjetja, z izjemo dogodkov razlikovanja/diskriminacije, v katere je vpletena vsaj ena notranja oseba.
- Zunanja goljufija

  Izgube zaradi vrste dejanj, katerih namen je poneverba, odtujitev lastnine ali izogibanje zakonodaji, s strani tretje osebe.
- Prakse v povezavi z zaposlovanjem in varnostjo pri delu

  Izgube, ki izhajajo iz dejanj, neskladnih z zakoni ali pogodbami, ki urejajo zaposlovanje, zdravje ali varnost, iz plačila odškodninskih zahtevkov v povezavi z osebnimi poškodbami ali iz dogodkov razlikovanja/diskriminacije.
- Stranke, produkti in poslovne prakse

  Izgube, ki izhajajo iz nenamernega neizpolnjevanja ali malomarnega izpolnjevanja strokovne obveznosti do določenih strank (vključno z zahtevami glede zaupnosti in ustreznosti poslovanja) ali iz narave ali sestave produkta.
- Škoda na premičnem in nepremičnem premoženju

  Izgube, ki izhajajo iz izgube ali poškodovanja premičnega in nepremičnega premoženja zaradi naravne nesreče in drugih dogodkov.
- Poslovne motnje in izpadi sistemov

  Izgube, ki izhajajo iz poslovnih motenj ali izpadov sistemov.
- Izvedba, dostava in upravljanje procesov

  Izgube, ki izhajajo iz neuspele obdelave poslov ali neuspelega upravljanja procesov, iz odnosov z nasprotnimi trgovskimi strankami in prodajalci.

Razen kategoriji »Prakse v povezavi z zaposlovanjem in varnostjo pri delu« in »Škoda na premičnem in nepremičnem premoženju« so ostale kategorije tesno povezane s kibernetskimi tveganji.

Baselske smernice iz junija 2011 za merjenje operativnega tveganja z naprednimi pristopi [1] določajo, da mora vsak napreden pristop temeljiti na uporabi štirih različnih skupin podatkov, in sicer:

- Notranji podatki (Internal loss data, ILD)
  Notranji podatki o izgubah predstavljajo oziroma izražajo profil poslovnega tveganja in način upravljanja banke. Notranji podatki o izgubah se uporabljajo v meritvenih sistemih za oceno porazdelitve izgub in oceni verjetnosti večjih izgub, prav tako pa tudi v stresnih scenarijih.

- Zunanji podatki (External Data, ED)
  Pri oceni verjetnosti resnih izgub in scenarijih mora banka uporabljati tudi uporabne podatke iz zunanjih javnih virov.

- Analiza scenarijev
  Različni scenariji omogočajo ocenitev stopnje izpostavljenosti banke operativnemu tveganju zaradi dogodkov, ki se zgodijo z majhno verjetnostjo, vendar lahko povzročijo visoke izgube.

- Dejavniki, ki odražajo poslovno okolje in notranje kontrole (ang. *Business environment and internal control factors, BEICF*)

Vključitev dejavnikov, ki odražajo poslovno okolje in notranje kontrole v model, vsekakor predstavlja izziv za banko. Omenjeni dejavniki se pogosto uporabljajo kot posredni vložek v model oziroma kot naknadna prilagoditev za model.

Banka mora skrbno pretehtati, na kakšen način bo vključila vse štiri podatkovne vire v napredni model merjenja operativnega tveganja, da se zagotovi sorazmernost med izračunom potrebnega kapitala in dejanskim tveganjem, ki mu je banka izpostavljena. Seveda mora banka znati utemeljiti izbiro pristopa ter imeti za to narejene ustrezne analize. Sama opredelitev naprednega modela za merjenje in izračun kapitalske zahteve za operativno tveganje ne določa natančne vrste modela in daje banki precejšnjo svobodo pri izdelavi lastnega modela. Seveda pa mora model zadostiti predvidenim kvalitativnim in kvantitativnim zahtevam. Najbolj pogosti napredni pristopi, ki jih banke uporabljajo za merjenje in izračun kapitalske zahteve za operativno tveganje, temeljijo na pristopu s statistično porazdelitvijo izgube (ang. *Loss Distribution Approach, LDA*), ki je postal standard v bančništvu [4]. S tem pristopom banka razdeli možne škodne dogodke po vrstah tveganj in poslovnih področij (z uporabo matrike poslovnih procesov) in za vsako kombinacijo oceni verjetnostno porazdelitev, na podlagi katere izračuna končno verjetnostno porazdelitev škodnih dogodkov za banko. Banka nato oceni kapitalsko zahtevo za operativno tveganje z metodo tvegane vrednosti (ang. *Value-at-Risk*). Tvegana vrednost napove največjo pričakovano izgubo banke na podlagi verjetnostne porazdelitve ob dani stopnji zaupanja (npr. 99,9 %) in časovnem obdobju (npr. eno leto).

3.4 Ostale metode za obvladovanje operativnega tveganja

Poleg obveznih pristopov za merjenje operativnega tveganja za namen izračuna kapitalske zahteve za operativna tveganja banke uporabljajo raznovrstne metode za merjenje in analiziranje operativnega tveganja.
V študiji »Problemi ocenjevanja in upravljanja z operativnimi tveganja v bankah« (ang. *Problems of evaluation and management of operational risks in banks*) [5], predstavljeni na mednarodni konferenci uporabne ekonomije julija 2015, so izpostavljene slabosti obstoječih pristopov in metod merjenja operativnega tveganja. Kot ena največjih pomanjkljivosti je izpostavljena odsotnost metodološkega okvira pri ocenjevanju negativnega učinka operativnega tveganja na poslovanje oziroma dobiček banke. Slednje je zelo težko analitično modelirati zaradi same narave operativnega tveganja.

Metode so odvisne od poslovnega modela banke oziroma tveganj, ki so jim banke izpostavljene. Banke imajo velik interes pravočasno identificirati tveganja ter se izogniti izgubam. Pri identifikaciji in analizi tveganj banke lahko razširijo vzorec škodnih dogodkov s potencialnimi škodnimi dogodki (ang. *near miss event*), ki se niso zgodili, vendar se je izkazalo, da je za to obstajala možnost. V splošnem lahko metode razdelimo na kvalitativne in kvantitativne. V nadaljevanju so predstavljeni še nekateri dodatni elementi in pristopi, ki so del učinkovitega upravljanja tveganj.

3.4.1 Samoocenitev tveganj

Z metodo samoocenitve tveganj (ang. *self-assessment*) banka oziroma posamezna področja banke sama ocenijo tveganja, katerim so oziroma katerim bi lahko bila izpostavljena. V primeru dobre oziroma kritične izvedbe samoocenitve je ta metoda zelo učinkovita, saj zaposleni na svojem področju najbolj poznajo tveganja, ki so jim izpostavljeni oziroma jih najhitreje zaznajo (npr. sumljivo delovanje aplikacij, nezadovoljstvo in užaljenost zaposlenih, možnost zlorab, tožb itd.).

3.4.2 Stresni scenariji

Stresni scenariji (ang. *scenario analysis*) so namenjeni analizi manj verjetnih dogodkov, vendar z velikimi izgubami za banko. Zaradi redkosti izjemnih dogodkov so le-ti po navadi spregledani v statističnih metodah, ki tudi sicer niso primerne za analizo stresnih dogodkov. Banka mora identificirati stresne scenarije, ki so verjetni, in biti na njih pripravljena.

3.4.3 Indikatorji tveganj

Banke lahko definirajo različne indikatorje, ki kažejo na različne vrste (potencialnih) operativnih tveganj oziroma škodnih dogodkov. Indikatorji lahko že relativno zgodaj opozarjajo na težave in omogočijo banki, da se pravočasno odzove. Indikatorji lahko na primer merijo: zadovoljstvo strank, število tožb, bolniško odsotnost, zadovoljstvo in preobremenjenost zaposlenih, število izpadov sistema, zlorab, kibernetskih napadov itd. Glavna prednost uporabe indikatorjev je, da lahko opozorijo na povečano verjetnost škodnih dogodkov še preden se zgodijo in omogočijo bankam pravočasno ukrepanje. Indikatorje se lahko smiselno vgradi v modele/sisteme za zgodnje odkrivanje (ang. *early warning systems*).

3.4.4 Kvantitativne metode

Kvantitativne metode lahko razdelimo na metode od zgoraj navzdol (ang. *top down*) in metode od spodaj navzgor (ang. *bottom up*). Metode od zgoraj navzdol običajno temeljijo na zgodovinskih podatkih ali na ocenah ekspertov. Med metodami od spodaj navzgor so se najbolj uveljavili pristopi s statistično porazdelitvijo izgube (ang. *loss distribution approach*), pristopi na podlagi scenarijev (ang. *scenario based approach*) in pristopi na podlagi dejavnikov tveganja in kontrol (ang. *risk drivers and controls approach*) [24]. Kvantitativne metode praviloma ocenjujejo tveganja s pomočjo verjetnostnih porazdelitev in ob izbrani stopnji zaupanja.

4 Tveganje informacijske tehnologije v bankah

Tveganje informacijske tehnologije (IT) je tveganje izgube dobička zaradi neustrezne informacijske tehnologije in procesov.

Tveganje informacijske tehnologije sodi v bančnem nadzoru v okvir operativnega tveganja, ki je zelo podrobno opredeljeno tako z vidika merjenja, upravljanja in spremljanja škodnih dogodkov, kot tudi z vidika izračunavanja kapitalskih zahtev.

Zaradi vse večje pomembnosti kibernetskega tveganja in njegovih zakonitosti v povezavi s kriminalnimi dejanji se ga v zadnjem obdobju še posebej spremlja.

Osnovne usmeritve glede tveganja informacijske tehnologije in varnosti informacij v bankah so podane v obstoječi bančni zakonodaji. V Sklepu o ureditvi notranjega upravljanja (33. člen) je zahtevano, da mora banka ustrezno omejiti dostop nepooblaščenim osebam do informacijskih sistemov z namenom varovanja zaupnih informacij in premoženja z uporabo ustrezne varnostne tehnologije ter da mora razvoj in zagotavljanje varnosti informacijskih sistemov ter informacij temeljiti na strategiji razvoja informacijskih sistemov in politiki varnosti informacijskih sistemov in informacij, ki vključuje: cilje pri zagotavljanju varnosti informacijskih sistemov in informacij, načela in postopke za varovanje zaupnosti, neoporečnosti in razpoložljivosti informacij ter porazdelitev odgovornosti glede varovanja informacijske tehnologije (strojne in programske opreme), informacij, shranjenih v informacijskih sistemih banke, ter pripadajoče dokumentacije [33].

Prav tako 33. člen Sklepa o ureditvi notranjega upravljanja določa, da morajo notranje kontrole pri informacijskih sistemih vključevati:

- Pri uresničevanju strategije razvoja informacijskih sistemov: ugotavljanje skladnosti s poslovnimi procesi, kvalitete projektnega načrtovanja, vključenosti ustreznih kadrov ter seznanjenosti različnih vodstvenih ravni s pripadajočo problematiko.
- Pri zagotavljanju varnosti informacijskih sistemov: logične in fizične kontrole pri dostopanju do informacijskih sistemov.
- Pri strojni opremi: ugotavljanje njene ustreznosti glede zahtev pripadajočih poslovnih procesov, notranjih in tehničnih standardov ter rednosti njenega vzdrževanja. Strojna oprema pomeni opredmeteno računalniško in komunikacijsko opremo.
- Pri programski opremi: ugotavljanje njene ustreznosti in uporabe v poslovnih procesih v smislu izpolnjevanja zahtev uporabnikov ter ločevanja funkcij razvoja, vzdrževanja in uporabe programske opreme. Programska oprema pomeni računalniške programe, postopke in pravila, ki zagotavljajo načrtovano operativnost strojne opreme.

4.1 Standardi na področju informacijske tehnologije

Trenutno ne obstaja enotna evropska bančna metodologija za ocenjevanje IT tveganja, zato je od nacionalnih nadzornih institucij odvisno, na katere standarde se zanašajo v povezavi z zahtevami, merjenjem in nadzorom ustreznosti informacijske tehnologije v bankah.

V Sklepu o dokumentaciji za izdajo dovoljenj za opravljanje bančnih in finančnih storitev ter za statusna preoblikovanja [32], ki ga je izdal svet Banke Slovenije 24. septembra 2015, je določeno, da mora banka, ki želi opravljati bančne storitve, imeti strategijo razvoja informacijskih sistemov in politiko varnosti informacijskih sistemov. Le-ta upošteva priporočila ustreznih standardov, ki jih izdaja Slovenski inštitut za standardizacijo (v nadaljevanju SIST) oziroma drug pooblaščeni organ.
Za ocenjevanje ustreznosti informacijske tehnologije in procesov se uporabljajo splošno uveljavljeni industrijski standardi. Med te standarde sodijo npr. okvir COBIT ali družina standardov ISO2700X.

4.1.1 COBIT

Kontrolni cilji za informacijsko in sorodno tehnologijo (ang. *Control Objectives for Information and Related Technologies, COBIT*) je mednarodno priznan okvir za standarde na področju informacijske tehnologije ter vodenja in upravljanja informacij in tehnologij. Vsebuje niz kontrol, urejenih v logične sklope. Prvo različico sistema COBIT je leta 1996 objavilo mednarodno neprofitno strokovno združenje ISACA (ang. *Information Systems Audit and Control Association*), ustanovljeno leta 1969. ISACA ima sedež v mestu Rolling Meadows (Illinois) v ZDA. Trenutno ima prek 140.000 članov iz 180 držav, organiziranih v 216 odsekih v 91 državah po vsem svetu. Slovenski odsek ISACA je bil na pobudo članov sekcije za revidiranje informacijskih sistemov pri Slovenskem inštitutu za revizijo (SIR) ustanovljen aprila 1995 kot 137. odsek te mednarodne organizacije [22].

4.1.2 ISO/IEC 2700X

ISO/IEC 2700X vključuje serijo standardov s področja informacijske varnosti, ki so bili izdani s strani Mednarodne organizacije za standardizacijo (ang. *International Organization for Standardization, ISO*) in Mednarodne elektrotehnične komisije (ang. *International Electrotechnical Commission, IEC*). ISO je neodvisna nevladna organizacija, ustanovljena leta 1947 s sedežem v Ženevi v Švici. Trenutno združuje nacionalne organizacije s področja standardizacije iz 163 držav. Iz Slovenije je član organizacije Slovenski inštitut za standardizacijo (SIST). IEC – Mednarodna elektrotehnična komisija je neprofitna, nevladna organizacija za standardiziranje, ki pripravlja in izdaja standarde na področju elektrotehnologije. Ustanovljena je bila leta 1906 in ima prav tako sedež v Ženevi. IEC sestavljajo polnopravne članice iz 60 držav in pridružene članice iz 23 držav. Iz Slovenije je polnopravna članica organizacije Slovenski inštitut za standardizacijo (SIST).

5 Kibernetsko tveganje

Zavedanje o kibernetskem tveganju postaja v zadnjem obdobju čedalje večje. Zaradi relativno novega področja je bilo pogosto nejasno, za kakšne vrste tveganja pravzaprav gre, kako ga definirati, identificirati, izmeriti obseg in učinek kibernetskih groženj in, seveda, kako ga v čim večji meri odpraviti oziroma nadzorovati.

V smernicah za kibernetsko odpornost infrastrukture finančnih trgov, ki sta jih pripravila Odbor za plačila in tržne infrastrukture (ang. *Committee on Payments and Market Infrastructures, CPMI)* pri Banki za mednarodne poravnave (*BIS*) in odbor Mednarodnega združenja nadzornikov trga vrednostnih papirjev (ang. *International Organization of Securities Commissions, IOSCO*), je kibernetsko tveganje definirano kot »kombinacija verjetnosti dogodka, ki nastane na področju informacij, računalniških in komunikacijskih sredstev organizacije in posledice tega dogodka za organizacijo« [3].

Kibernetsko tveganje se je povečalo zaradi razvoja informacijske tehnologije, pametnih naprav in naprednih načinov komunikacije. Zaradi spremenjenega oziroma naprednega delovanja podpornih sistemov in procesov se je spremenila tudi njihova varnost in stabilnost. Če so bili v preteklosti vzpostavljeni mehanizmi za učinkovito hranjenje dokumentov in dragocenih stvari ali gotovine v trezorjih, v fizično zelo težko dostopnih prostorih, se je z digitalizacijo učinkovitost in stabilnost mehanizmov bistveno spremenila. Ko govorimo o samih kriminalnih dejanih (ang. *Cybercrime*), gre vsebinsko v bistvu pravzaprav za stare vrste kriminalnih dejanj, pri čemer se uporabljajo nove (informacijske) tehnologije. Tako kazniva dejanja, kot so kraja (intelektualne) lastnine, zaupnih informacij, kraja identitete, uničevanje lastnine, izsiljevanje, razkrivanje zaupnih informacij, vohunjenje samo po sebi, niso nič novega, vendar v tehnološko spremenjenih okoliščinah dosežejo povsem nove razsežnosti. V mnogih primerih ne gre za kibernetski kriminal, povezan z neposrednim oškodovanjem posameznikov oziroma organizacij, pač pa gre lahko za prikrito vplivanje na obnašanje posameznikov ali organizacij ali pa gre za pridobivanje informacij, ki lahko prinašajo velike finančne koristi.

Že zdavnaj so minili časi, ko so se s spletnimi prevarami in s kriminalom ukvarjali večinoma posamezniki, pogosto z ne najbolj jasnimi nameni in cilji. Dandanašnji kibernetski kriminalci so visoko motivirani profesionalci, ki so pogosto financirani s strani premožnih kriminalnih organizacij ali celo držav. Imajo jasne cilje in strategijo, zaradi česar so mnogo bolj vztrajni in potrpežljivo čakajo na ranljivosti, ki se pojavijo. Ranljivosti informacijskih struktur načrtno raziskujejo in pri tem uporabljajo najbolj sofisticirano programsko opremo oziroma napredne računalniške viruse.

Pri obravnavi kibernetske varnosti je potrebno omeniti tudi problematiko ogrožanja temeljnih svoboščin, pridobljenih v razvitem svetu, kot so pravica do zasebnosti in zaupnosti informacij. Le-te niso ogrožene le s strani kibernetskih kriminalcev, pač pa tudi s strani institucij, ki za učinkovito obrambo pred kibernetskimi nevarnostmi potrebujejo dostope do vse več osebnih podatkov in značilnosti posameznikov.

5.1 Najresnejše kibernetske grožnje v letu 2015

Kibernetske grožnje se zaradi hitrih sprememb informacijske tehnologije, uporabe pametnih naprav, načina komunikacije in navad uporabnikov ter iznajdljivosti kibernetskih kriminalcev neprestano spreminjajo.

Po podatkih enega vodilnih podjetij na področju protivirusne zaščite Kaspersky Lab je bilo v letu 2015 zlonamerni programski opremi izpostavljenih 58 %, spletnemu napadu pa 29 % vseh poslovnih računalnikov [23].

Kadar gre za visoko motivirane in dolgotrajnejše napade na določeno tarčo, govorimo o naprednih in dolgotrajnih grožnjah (ang. *Advanced Persistent Threat*). V takih primerih gre običajno za politične ali gospodarske motive in ozadja, odkriti pa so lahko šele po nekaj mesecih ali celo letih.

Obstaja tudi korelacija med tarčami napadalcev in vrstami napadov. Tarče kibernetskega vohunjenja (ang. *cyber espionage*) so npr. predvsem vlade, strateške državne ustanove in medijske hiše, medtem ko je v primeru napada na banke oziroma bančne kriminalitete pogost napad z zlonamerno programsko opremo s ciljem kraje identitete, prestrezanja informacij in prevzema oddaljenega nadzora.

V nadaljevanju so predstavljene glavne značilnosti najresnejših kibernetskih groženj v letu 2015 po podatkih Evropske agencije za varnost omrežij in informacij (ang. *European Union Agency for Network and Information Security*, v nadaljevanju ENISA) [15].

5.1.1 Zlonamerna programska oprema (ang. *Malware*)

Zlonamerna programska oprema je največja kibernetska grožnja v zadnjih letih. Gre za zlonamerno programsko opremo, nameščeno v računalniških sistemih z namenom izvrševanja nelegalnih aktivnosti. Lahko gre za uničevanje podatkov, nepooblaščen dostop oziroma vohunjenje ali za oddaljen prevzem nadzora nad okuženimi računalniki. Glede na način razširjanja jih poimenujemo tudi virusi (programi, ki se razširjajo skupaj z nameščanjem drugih programov), črvi (razširjajo se samostojno) in trojanskimi konji, ki se ne razširjajo samodejno, pač pa se namestijo skupaj z okuženim programom ter omogočajo prevzem nadzora na daljavo.

Napredna pristopi nameščajo zlonamerno programsko opremo na samo strojno opremo, kot so razne interne kartice, USB ključki, prenosni diski itd. Dober primer je delovanje zelo napredne skrivnostne vohunske skupine, poimenovane »*Equation group*«, ki uporablja strojno reprogramiranje (ang. *hardware re-programming*), ki omogoča nameščanje zlonamernih informacij (npr. spletnih naslovov) v sistemsko programsko opremo trdega diska. Tak način okužbe je težko zaznati in odstraniti, saj je odporen na formatiranje diska ali na ponovno namestitev operacijskega sistema. Tako okuženo strojno opremo je pogosto potrebno v celoti nadomestiti.

V porastu je tudi mobilna zlonamerna programska oprema (v letu 2015 je bila njena rast 50 %). Na področju mobilnih zlonamernih programov do okužb najpogosteje prihaja z direktno (ročno) namestitvijo škodljivih programov, zatem sledi namestitev zlonamerne kode v obliki lažne ponudbe in nato namestitev zlonamerne kode preko zavajajočih povezav do zlonamernih spletnih strani. Najbolj so izpostavljene mobilne naprave z operacijskim sistemom Android, ki imajo več kot 95 % delež mobilnih zlonamernih programov.

Pri zlonamerni programski opremi je problematična predvsem dostopnost orodij, ki omogočajo, da tudi tehnično neizkušeni uporabniki razvijajo svoje lastne različice zlonamernih programov. Še vedno pa se zlonamerna programska oprema najbolj širi po najenostavnejših metodah, kot so makroji v MS Office dokumentih, ki naložijo in namestijo zlonamerno programsko opremo. Drugi najpogostejši način širjenja poteka preko zlorabe družbenih socialnih omrežij, predvsem preko usmerjanja na spletne naslove z okuženo vsebino.

5.1.2 Napadi na terminale na prodajnih mestih (ang. *Attacks on POS terminals*)

Terminali na prodajnih mestih oziroma POS (ang. *Point of sale*) terminali so naprave, ki omogočajo uporabo plačilnih kartic na fizičnem prodajnem mestu. Vsak računalnik, ki je povezan s čitalnikom branja plačilnih kartic, je potencialna tarča napadalcev. Okužen računalnik z dostopom do čitalnika kartic lahko opravlja funkcijo POS terminala. Napadalci se trudijo pridobiti podatke o kartici, s katerimi lahko nato v škodo uporabnikov kartic izvršujejo plačila.

5.1.3 Spletni napadi (ang. *Web-based attacks*)

Spletni napadi uporabljajo spletne strani za širjenje in nameščanje zlonamerne kode. Napadalci se osredotočajo na spletne strežnike in odjemalce. Spletni napadi zajemajo zlonamerne spletne naslove, identificiranje in okuževanje priljubljenih spletnih mest (ang. *watering hole attack*), poskuse nameščanja kode neposredno s spletne strani (ang. *drive-by attack*), skrite prevzeme nadzora nad spletno stranjo (ang. *web backdoor*) in napade na brskalnike. Napad na brskalnike pogosto poteka preko nameščanja vtičnikov/dodatkov v brskalniku.

Ključni element spletnih napadov ostajajo zlonamerni spletni naslovi, ki so okuženi z zlonamernimi programi oziroma ki preusmerjajo na zlonamerne spletne strani z namenom okužbe naprav končnih uporabnikov. Poleg nezaželene oglaševalske programske opreme (ang. *Adware-advertising-supported software*), ki jih širi avtor z namenom ustvarjanja prihodka, se ravno preko spletnih naslovov najpogosteje širi zlonamerna programska oprema. Spletni napadi naraščajo zlasti zaradi vedno večje vloge prevar na socialnih omrežjih.

Za preprečevanje spletnih napadov je priporočljivo filtriranje prometa na spletnem brskalniku z namenom odkrivanja skritih spletnih napadov. Priporočljivo je rangiranje spletnih naslovov, spletnih vsebin, datotek in aplikacij po ugledu ter preverjanje tako imenovanega črnega seznama sumljivih spletnih strani. Prav tako je na mestu pazljivost nameščanja funkcij spletnih brskalnikov, če te niso nujne za poslovanje.

5.1.4 Napadi na spletne aplikacije (ang. *Web application attacks*)

Zaradi porasta spletnih aplikacij so napadi nanje čedalje pogostejši. Več komponent kot jih uporabljajo spletne aplikacije, več je možnosti za napad. Med to vrsto napadov sodijo vrivanje programske kode na spletno stran (ang. c*ross-site scripting, XSS*) in napadi na zbirke podatkov ob pomoči vrivanja SQL stavkov. Nameni so lahko pridobivanje/kraja podatkov, nameščanje zlonamerne kode, zloraba prenesenih podatkov, uhajanje podatkov, zloraba ranljivosti ter izogibanje pogojem in zahtevam pri spletnem nakupovanju. Napadi na spletne aplikacije so torej pomembno orodje za vrivanje zlonamernih programov, pa tudi za uhajanje informacij in kršitve varnosti podatkov. Napad se pogosto izvaja s pomočjo programov, ki so že nameščeni na spletni strani (ang. *local file inclusion*, *LFI*).

5.1.5 Omrežje okuženih računalnikov – botnet omrežja (ang. *Botnet*)

Botnet omrežja so ena najpomembnejših infrastrukturnih komponent za širjenje različnih vrst kibernetskih napadov. Sestavljajo jih veliko število med seboj povezanih računalnikov bodisi preko centralnega strežnika bodisi pri medsebojni povezanosti vseh računalnikov (ang. *peer to peer*). Napadalci nato prevzamejo nadzor nad večjim številom okuženih računalnikov (lahko nekaj sto tisoč) in nato izvršijo usklajen napad.

Zaradi pomembnosti za kibernetski kriminal so botnet omrežja v središču pozornosti. Globalno usklajeno odstranjevanje s strani organov pregona je prispevalo k upadanju te grožnje. Najpogosteje se uporablja botnet omrežje za pošiljanje nezaželene pošte ali za obremenitveni napad na določeno spletno stran. Na sivem trgu se je razvila tudi trgovina z botnet omrežji, saj nekateri prodajajo nadzor nad botnet omrežjem za določen čas.

5.1.6 Ohromitev delovanja storitev (ang. *Distributed denial of service, DDoS*)

Ohromitev delovanja storitev oziroma porazdeljeni napadi onemogočanja je pomembno orodje v rokah kibernetskih kriminalcev. Napad se zgodi tako, da napadalci pošljejo ogromno količino zahtev na strežnik, ki zaradi preobremenjenosti odpove. Pričakuje se, da bodo tovrstne grožnje še naraščale, napadalne taktike pa bodo vedno bolj učinkovite. Podaljšuje se tudi trajanje napadov. Napadalci uporabljajo omrežje botnet ali omrežne usmerjevalnike. Razvoj interneta stvari (ang. *Internet of Things –IoT*) oziroma vse večje povezovanje pametnih naprav preko omrežja ali interneta še dodatno prispeva k nevarnosti napadov z namenom ohromitve delovanja storitev, saj v takih okoljih lahko prihaja do zlorab pri uporabi komunikacijskih protokolov. Napadalci za zaustavitev porazdeljenih napadov onemogočanja (DDoS), ki so jih sprožili proti organizaciji, pogosto zahtevajo tudi odkupnino.

5.1.7 Notranja grožnja (ang. *Insider threat*)

Notranje grožnje ostajajo pomembna nevarnost, saj je približno tretjina varnostnih incidentov v

kibernetskem prostoru posledica nenamernih in namernih dejavnosti posameznikov, ki imajo dostop do notranjih informacij. Incidente je pogosto težko razlikovati med nepremišljenimi, zmotnimi in namernimi dejavnostmi oseb z notranjimi informacijami. Ob povišani stopnji kibernetskega vohunjenja in socialnega inženiringa notranje grožnje odpirajo široke možnosti izkoriščanja raznovrstnih načinov zlorabe, ki temeljijo na notranjih informacijah. Nevarnosti izhajajo s strani zaposlenih, nekdanjih zaposlenih in pogodbenih strank, ki imajo ali so imeli dostop do zaupnih podatkov in želijo zaradi različnih interesov škodovati podjetju.

5.1.8 Neželena pošta (ang. *Spam*)

Neželena elektronska pošta je ena najstarejših kibernetskih groženj. Še vedno ostaja osnovno orodje storilcev kibernetskih kaznivih dejanj. Čeprav ne gre za napredno tehnologijo in njena uporaba že nekaj let upada, ostaja nezaželena pošta še vedno pomembno in učinkovito sredstvo prenosa zlonamernih programov. Okrog 6 % vse neželene pošte prenaša zlonamerne priponke ali povezave. Nezaželena pošta se pogosto opira na različne dogodke in prireditve, da lažje najde pot do naslovnikov. Upadanje števila neželenih oglasnih sporočil je posledica odstranjenih botnet omrežij in učinkovitega filtriranja pošte in naslovov, ki so jih delodajalci in vladne agencije uvrstili na črni seznam.

5.1.9 Ribarjenje (ang. *Phishing*)

Ribarjenje je kraja podatkov, pri kateri napadalci zavajajo žrtve tako, da jih zvabijo na lažno spletno stran, ki se zdi znana in vredna zaupanja. Nato od nič hudega sluteče žrtve pridobijo občutljive podatke (uporabniška imena, gesla) oziroma žrtve prepričajo, da namestijo (zlonamerno) programsko opremo pod pretvezo, da je nujna oziroma del rednega servisiranja. Glavni namen ribarjenja je kraja podatkov ali namestitev zlonamerne programske opreme na napravo žrtve. Ribarjenje je neke vrste napredna oblika neželene pošte, saj je ciljno usmerjena in tako potencialno učinkovitejša. V smislu infrastrukture, prek katere se izvaja, ima veliko skupnega z neželeno pošto. Da se vzpostavi lažno zaupanje, ribarjenje uporablja dogodke, ki so znani iz novic oziroma poskuša posnemati zaupanja vredne organizacije, blagovne znamke, storitve, osebe in podobno.

5.1.10 Paket zlonamernih programov (ang. *Exploit kit*)

Paketi zlonamernih programov so bili razviti v zadnjem obdobju in so že prevzeli vodilni položaj med kibernetskimi grožnjami. So orodje za razširjanje zlonamernih programov. Paketi so nameščeni na strežnikih in sistematično zbirajo informacije o uporabnikih ter preverjajo ranljivost v brskalnikih uporabnikov in na njih nameščajo ustrezno zlonamerno programsko opremo, ki jo lahko izkoriščajo. Na črnem trgu se nato ponujajo storitve (nameščanja zlonamernih programov) na že okužene računalnike oziroma se prodaja celoten paket. Pogosto razvijalci paketa zlonamernih programov tesno sodelujejo s kupci (ki uporabljajo pakete za svoja kriminalna početja) in glede na njihove potrebe izpopolnjujejo pakete. Danes so eno

glavnih orodij nameščanja zlonamernih programov. Poleg vzpostavitve ustrezne infrastrukture za medsebojno delovanje zlonamernih orodij se tako vzpostavlja tudi človeško infrastrukturo, ki je sposobna nenehno izpopolnjevati metode in orodja napadov.

5.1.11 Kršitve varnosti podatkov (ang. *Data breaches*)

Kršitve varnosti podatkov so posledica uspešnih poskusov ogrožanja zaupnih informacij, to je tistih informacij, ki jih organizacije varujejo in ki so pomembne za njihovo poslovanje. V kontekstu kibernetskega prostora so kršitve varnosti podatkov izgube podatkov, do katerih prihaja zaradi povzročiteljev kibernetskih groženj. Kršitve varnosti podatkov se intenzivno obravnavajo v kontekstu drugih kibernetskih groženj.

5.1.12 Kraja identitete (ang. *Identity theft*)

Kraja identitete je poseben primer kršitve varnosti podatkov. Gre za krajo vseh vrst identitet oziroma informacij o identiteti uporabnikov. Primeri zlorab so raznovrstni. Poverilnice (ang. *credentials*) omogočajo dostop do storitev in podatkov, ki se jih lahko zlorabi. Podatki o identiteti se lahko uporabijo pri ustvarjanju uporabniških profilov in podobno. Ta grožnja predstavlja potrošniško stran kršitev varnosti podatkov in je še posebej pomembna, ker lahko njena zloraba neposredno vpliva na stranke, ki bodo sčasoma morale tudi poskrbeti za korektivne ukrepe.

Glede na vse večjo uporabo informacij o identiteti na mnogih pomembnih področjih življenja, kot so zdravstvo, finance, energija in transport, lahko uporabniki utrpijo veliko škodo, če pride do zlorabe njihovih osebnih podatkov.

Do kršitve varnosti podatkov in kraje identitete lahko pride z uhajanjem informacij, ribarjenjem ali zlonamernimi programi. Med osebne podatke sodijo imena, priimki, naslov, e-poštni naslovi, identifikacijske številke osebnih dokumentov (npr. osebna izkaznica, potni list, vozniško dovoljenje, članska izkaznica), naslov IP, številka registrske tablice, davčna številka, številke kreditnih kartic, digitalna identiteta, datum rojstva, rojstni kraj, telefonska številka, zdravstvene informacije itd.

5.1.13 Uhajanje informacij (ang. *Information leakage*)

Pri uhajanju informacij gre za neopazno razkrivanje majhnega števila informacij z zlorabo tehničnih sistemov ali z goljufivimi aktivnostmi. Uhajanje informacij je kršitev varnosti podatkov posameznih evidenc oziroma zadeva majhno količino informacij, ki pa so pomembne. Uhajanje informacij se obravnava na drugačen način kot kršitve varnosti podatkov, saj se ukradene informacije ne le po obsegu, ampak tudi po kakovosti razlikujejo od kršitve varnosti podatkov. Slabosti, ki se izrabljajo pri uhajanju informacij, so običajno povezane z nepravilnim delovanjem tehničnih komponent ali funkcij aplikacij. Grožnja uhajanja informacij vodi h kraji osebnih podatkov in poverilnic. Te se lahko uporabijo za prevare,

nameščanje zlonamernih programov, zlorabo in kršitve varnosti podatkov. Uhajanje informacij lahko prispeva k zbiranju velikih količin osebnih ali zaupnih podatkov (vključno s poverilnicami), ki imajo veliko vrednost tudi izven črnih trgov.

5.1.14 Izsiljevalski programi (ang. *Ransomware*)

Izsiljevalski programi so dosegli svoj razmah v letu 2015, ko so se napadi z njimi skoraj podvojili. Izsiljevalski programi ciljajo na državljane, ki naj bi bili bolje situirani, torej večinoma iz Severne Amerike in Evrope. Izsiljevalski programi najpogosteje zakodirajo računalnike oziroma jih kako drugače onemogočijo nato pa napadalci zahtevajo plačilo odkupnine za posredovanje kode, ki omogoči dostop do podatkov oziroma jih dešifrira.

5.1.15 Kibernetsko vohunjenje (ang. *Cyber espionage*)

Kibernetski prostor postaja bojno polje prihodnosti. Nacionalne države so glede kibernetskih zmogljivosti trenutno v oboroževalni tekmi. Kibernetsko vohunjenje narašča in se izpopolnjuje. Aktivno podpiranje držav pri razvijanju programske opreme za vohunjenje odpira popolnoma nove dimenzije zaradi tehnologije, znanja in sredstev, ki so na voljo.

5.2 Odmevni napadi na banke v letu 2015

Najodmevnejši napadi na banke v Sloveniji so se dogajali januarja 2015. Napadenih je bilo šest bank, in sicer z uporabo ribarjenja (ang. *Phishing*). Napadalci so pridobili elektronske naslove komitentov bank in nato na njihove naslove pošiljali elektronska sporočila s povezavo do lažnih spletnih strani bank, ki so bile na pogled zelo podobne originalnim stranem. Preko lažnih spletnih strani so napadalci poskušali pridobiti gesla za dostop do elektronskega bančništva. Napadi so trajali dober teden. H končanju napadov je prispevalo obveščanje javnosti in ukrepanje pristojnih organov. Osrednji nacionalni organ za obravnavo kibernetskega tveganja Center SI-CERT ocenjuje, da je bilo poslanih približno 100.000 lažnih sporočil in postavljenih približno 40 lažnih kopij spletnih mest bank.

V tujini je v letu 2015 najbolj odmeval napad, ki ga je izvedla skupina, poimenovana Carbanak [23]. Po podatkih Kaspersky Lab je bilo v dveh letih napadenih okrog 100 finančnih institucij iz 30 držav po vsem svetu, znesek ukradenega denarja pa je znašal blizu milijarde dolarjev. Napad je bil eden največjih v zgodovini in je presenetil vse. Napadalci so kradli denar neposredno bankam in ne komitentom. Napadalci so uporabljali tehniki ribarjenja (ang. *phishing*) in stranskih vrat (ang. *backdoor*), s pomočjo katerih so prevzeli nadzor nad računalniki. Najprej so uporabljali tehniko usmerjenega ribarjenja, s tem da so bančnim uslužbencem pošiljali lažniva elektronska sporočila z zlonamerno programsko opremo. Ko so okužili računalnike, ki so jih uporabljali bančni uslužbenci, so lahko na daljavo spremljali vsako njihovo aktivnost, s čimer so prišli do ključnih podatkov. Pridobili so dostop do omrežja in do ključnih administrativnih

računalnikov v banki. Okuženi računalniki so mesece dolgo pošiljali podatke napadalcem, vključno z videoposnetki in s fotografijami. Sčasoma so napadalci lahko v celoti prevzeli identiteto bančnih uslužbencev in se zelo dobro seznanili z delovanjem bančne programske opreme. Šele kasneje so pričeli aktivno upravljati programsko opremo in pričeli z nakazili na račune bank v tujini, zaradi česar dolgo nihče v banki in nihče od komitentov ni posumil, da se dogaja nekaj nenavadnega. Pri tem so napadalci skrbno prikrivali svoje sledi. Ko so iz določenega računa nakazali znesek v tujino, so stanje na računu popravili na prvotno stanje, da komitenti niso opazili spremembe stanja na računu. V povprečju so posamezno banko oškodovali za 2,5 do 10 milijonov dolarjev. Uspelo jim je prevzeti tudi nadzor nad bankomati. Najbolj nenavaden način kraje je potekal preko okuženih (daljinsko nadzorovanih) bankomatov, ki so na ukaz ob točno določenem času nenadoma pričeli izplačevati gotovino.

5.3 Incidenti v Sloveniji

Osrednji nacionalni organ za obravnavo kibernetskega tveganja Center SI-CERT je v letu 2015 obravnaval 732 incidentov, povezanih s tehničnimi napadi, in 901 incidentov, povezanih s spletnimi goljufijami [31].

Incidente, povezane s tehničnimi napadi, največkrat povzročijo virusi, ki se širijo preko priponk v elektronskih poštah in pri prenašanju datotek s spleta.

Tabela 1: Tehnični napadi – Obravnavani incidenti v Sloveniji

Vrsta incidenta/Leto	2008	2009	2010	2011	2012	2013	2014	2015
Pregledovanje omrežja	86	39	44	62	51	43	65	65
Botnet	9	3	11	12	12	16	13	17
Napad onemogočanja (DDoS)	22	10	18	28	47	76	124	94
Škodljiva koda	18	53	68	126	258	417	438	418
Zloraba storitve	16	15	12	28	9	8	9	15
Vdor v sistem	32	25	56	93	76	61	32	43
Zloraba up. računa				1	9	37	60	40
Razobličenje					125	80	167	33
Napad na aplikacijo					17	22	33	7
Skupaj – tehnični napadi	**183**	**145**	**209**	**350**	**604**	**760**	**941**	**732**

Vir: Poročilo o omrežni varnosti za leto 2015, SI-CERT.

Pri spletnih goljufijah je v zadnjih letih izjemno opazen naraščajoč trend. Pri goljufijah pogosto ne gre za uporabo sofisticirane programske opreme. Goljufije pogosto bolj odražajo trende obnašanja tako napadalcev kot žrtev. Pri goljufijah napadalci običajno stopajo v stik z žrtvami preko spletnih servisov oziroma preko popularnih družbenih omrežij.

Največje posamično oškodovanje v letu 2015 v Sloveniji je bilo v višini 18.000 EUR, in sicer v obliki Nigerijske prevare (sporočilo, s katerim napadalec prepriča žrtev, da mu nakaže denar). Ostala večja finančna oškodovanja so se zgodila preko lažnega predstavljanja, ko so napadalci spremljali elektronsko korespondenco med podjetji in nato v nekem trenutku poslali elektronsko pošto pod krinko podjetja, vendar z lažnim bančnim računom, kamor naj bi se nakazala kupnina oziroma plačilo za opravljene storitve.

Tabela 2: Goljufije in prevare – obravnavani incidenti v Sloveniji

Vrsta incidenta/leto	2008	2009	2010	2011	2012	2013	2014	2015
Kraja identitete			10	52	67	56	77	70
Nigerijska (419) prevara							38	26
Spletno nakupovanje							68	88
Druge goljufije	5	24	26	89	161	210	309	322
Neželena pošta (ang. *Spam*)	21	22	36	25	74	50	63	112
Ribarjenje (ang. *Phishing*)	23	38	50	61	139	209	279	283
Klicalniki (ang. *Dialer*)					1		3	
Skupaj – goljufije in prevare	**49**	**84**	**122**	**227**	**442**	**525**	**837**	**901**

Vir: Poročilo o omrežni varnosti za leto 2015, SI-CERT.

5.4 Trenutni položaj kibernetske varnosti v Evropski uniji

Povečano število kibernetskih napadov, vse večja odvisnost od naprednih tehnologij in politične napetosti v svetu so pripomogle k temu, da so države ter vojaške zveze v zadnjih letih kibernetsko varnost uvrstile zelo visoko med svoje prioritetne naloge.

Ni presenetljivo, da je varnost pred spletnimi napadi in kriminalom ena izmed osrednjih determinant zaupanja potrošnikov in spletnega gospodarstva.

Strategija kibernetske varnosti Evropske unije (ang. *Cybersecurity Strategy for the European Union*) [16], Direktiva o varnosti omrežij in informacij (ang. *Directive on security of network and information systems*, v nadaljevanju Direktiva NIS) [7] in Evropska agenda za varnost (ang. *European Agenda on Security*) [17] predstavljajo strateško ogrodje EU na področju kibernetske varnosti in kriminala.

Strategija kibernetske varnosti Evropske unije je bila objavljena 7. februarja 2013 z naslovom »Odprt, varen in zavarovan kibernetski prostor« in predstavlja usmeritev EU pri soočanju s kibernetskimi nevarnostmi. S posebnimi ukrepi naj se bi okrepila kibernetska odpornost informacijskih sistemov, zmanjšal kibernetski kriminal ter okrepili mednarodna politika EU za kibernetsko varnost in kibernetska obramba EU.

Tri leta je trajalo, da sta se Evropski parlament in Evropski svet dogovorila o nizu ukrepov za povečanje splošne ravni kibernetske varnosti v EU in da je Evropski parlament 6. julija 2016 sprejel Direktivo NIS. Direktiva NIS je prvi del evropske zakonodaje na področju kibernetske

varnosti in zagotavlja pravni okvir in ukrepanje za povečanje splošne ravni kibernetske varnosti v EU. Direktiva NIS je stopila v veljavo avgusta 2016. Države članice EU morajo določbe direktive prenesti v nacionalno zakonodajo v enaindvajsetih mesecih.

Da kibernetska kriminaliteta pridobiva na pomenu, je razvidno tudi iz Evropske agende za varnost za obdobje 2015–2020 [18], ki jo je Evropska komisija predstavila in sprejela 28. aprila 2015 in katere cilj je podpirati sodelovanje držav članic pri odpravljanju varnostnih groženj in krepiti skupna prizadevanja v boju proti terorizmu, organiziranemu kriminalu ter kibernetski kriminaliteti. Agenda opredeljuje boj proti kibernetski kriminaliteti poleg preprečevanja terorizma in boja proti radikalizaciji ter boja proti organiziranemu kriminalu kot eno od glavnih groženj za evropsko varnost.

Dejavnosti na področju varnosti omrežij in informacij so podprte s strani Evropske agencije za varnost omrežij in informacij (ENISA) ter skupine za odzivanje na računalniške grožnje (ang. *Computer Emergency Response Team,* v nadaljevanju CERT-EU) za institucije EU.

5.4.1 Evropska agencija za varnost omrežij in informacij (ENISA)

Evropska agencija za varnost omrežij in informacij (ang. *European Union Agency for Network and Information Security*, *ENISA*) je strokovni center za kibernetsko varnost v Evropi. Agencija se nahaja v Grčiji s sedežem v Heraklionu na Kreti in z operativnim uradom v Atenah. ENISA je bila ustanovljena leta 2004 in aktivno prispeva k visoki ravni varnosti omrežij in informacij v EU ter k razvoju kulture in k ozaveščanju o pomenu varnosti omrežij in informacij v EU. ENISA tesno sodeluje z državami članicami in z zasebnim sektorjem pri zagotavljanju ustreznih nasvetov in rešitev. To vključuje vseevropske kibernetske vaje (ang. *Pan-European Cyber Security Exercises*) in sodelovanje pri razvoju nacionalnih strategij za kibernetsko varnost. ENISA podpira razvoj in izvajanje politike in zakonodaje Evropske unije o zadevah v povezavi z omrežno in informacijsko varnostjo.

5.4.2 CERT-EU

Stalno skupino za odzivanje na računalniške grožnje za institucije EU (ang. *Computer Emergency Response Team,* CERT-EU) so 11. septembra 2012 ustanovile Institucije EU. Sestavljajo jo IT varnostni strokovnjaki iz vseh glavnih institucij EU (Evropska komisija, generalni sekretariat Sveta, Evropski parlament, Odbor regij, Evropski ekonomsko-socialni odbor). CERT-EU tesno sodeluje z drugimi sorodnimi skupinami CERT v državah članicah EU kot tudi s specializiranimi podjetji s področja informacijske varnosti.

5.4.3 Europol

Osrednja institucija, ki se na ravni EU ukvarja s kibernetskim kriminalom na operativni ravni, je Europol, in sicer v okviru svojega Evropskega centra za kibernetsko kriminaliteto (ang. *European Cybercrime Centre*).

5.5 Trenutni položaj kibernetske varnosti v Sloveniji

5.5.1 Center SI –CERT

Slovenska skupina za odzivanje na računalniške grožnje (ang. *Slovenian Computer Emergency Response Team,* v nadaljevanju SI-CERT) je slovenski nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij, ki od leta 1995 deluje v okviru javnega zavoda Arnes. Trenutno je osrednji nacionalni organ za obravnavo kibernetskega tveganja. Center ima vpogled v trende, v podatke o sorodnih incidentih doma in v tujini, s čimer nato v primeru posameznih incidentov s svojim specializiranim znanjem in izkušnjami izboljšuje in pospešuje razreševanje aktualnih primerov v Sloveniji.

Opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah v elektronskih omrežjih. Trenutno opravlja tudi naloge Vladnega centra za odzivanje na omrežne incidente (SIGOV-CERT) in pomaga pri vzpostavitvi samostojnega centra, ki bo skrbel za zaščito informacijske infrastrukture državne uprave. SI-CERT je član svetovnega združenja odzivnih in varnostnih centrov FIRST (ang. *Forum of Incident Response and Security Teams*), član skupine nacionalnih odzivnih centrov pri CERT/CC, član delovne skupine evropskih odzivnih centrov TF-CSIRT in je akreditiran v programu Trusted Introducer. SI-CERT je slovenska kontaktna točka za Varnostni organ Generalnega sekretariata Sveta EU in nacionalna informacijska točka za program IMPACT (ang. *International Multilateral Partnership Against Cyber Threats*) mednarodne telekomunikacijske zveze (ang. *International Telecommunication Union, ITU*). Storitve odzivnega centra SI-CERT so na voljo širši javnosti. SI-CERT se financira iz sredstev, ki jih za javni zavod Arnes zagotavlja Direktorat za informacijsko družbo Ministrstva za izobraževanje, znanost in šport. V letu 2015 so sodelavci centra SI-CERT opravili 40 predavanj in predstavitev o kibernetski varnosti in varni uporabi interneta [30].

5.5.2 Sprejete strategije in politike na področju kibernetskega tveganja

V Sloveniji so bili ključni strateški dokumenti, ki urejajo področje kibernetske varnosti, sprejeti v začetku leta 2016. Dne 25. 2. 2016 je Vlada RS sprejela Strategijo kibernetske varnosti [39]. Nekaj dni kasneje dne 10. 3. 2016 pa je sprejela strategijo Digitalna Slovenija 2020 – Strategija razvoja informacijske družbe do leta 2020 [37] in Načrt razvoja širokopasovnih omrežij naslednje generacije do leta 2020 [38].

S sprejetimi dokumenti so vzpostavljene strateške usmeritve razvoja informacijske družbe do leta 2020. Z Strategijo kibernetske varnosti Slovenija želi okrepiti svoj sistem za zagotavljanje kibernetske varnosti ter to področje tudi sistemsko urediti. Strategijo kibernetske varnosti je precej splošna zato obstaja možnost, da ne bo udejanjena v celoti. Slednje je predvsem odvisno od zavedanja kibernetske ogroženosti, splošne varnostne kulture ter politične volje.

Trenutno so operativne zmogljivosti za odzivanje na kibernetske grožnje porazdeljene med

naslednje institucije oziroma organe:

- Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (SI-CERT),
- Sektor za informacijsko varnost v okviru Direktorata za informatiko na Ministrstvu za javno upravo,
- Sistemi na področju obrambe in varstva pred naravnimi in drugimi nesrečami v okviru Ministrstva za obrambo,
- Področje protiobveščevalnega delovanja v okviru agencije SOVA,
- Urad za informatiko in telekomunikacije v okviru policije,
- Center za računalniško preiskovanje v okviru kriminalistične policije.

V analizi obstoječega stanja v Strategiji kibernetske varnosti je navedeno: »razen policije, ki je v zadnjih petih letih izboljšala svoje kapacitete za preiskovanje in preprečevanje kibernetske kriminalitete, so drugi organi podhranjeni na kadrovskem, materialno-tehničnem in organizacijskem področju. Kljub pomanjkljivostim, zmogljivosti na operativni ravni obstajajo, ne obstaja pa koordinacijsko telo, ki bi na strateški ravni povezovalo navedene deležnike« [39].

Med ukrepi, ki jih predvideva Strategija kibernetske varnosti, sta sicer tudi vzpostavitev osrednje koordinacije nacionalnega sistema zagotavljanja kibernetske varnosti ter njena kadrovska in tehnološka okrepitev skupaj z vzpostavitvijo samostojnega odzivnega centra za sisteme v javni upravi (SIGOV-CERT).

V skladu s Strategijo kibernetske varnosti bodo na operativni ravni zagotavljanja kibernetske varnosti s svojimi zmogljivostmi delovali SI-CERT na nacionalni ravni, Ministrstvo za obrambo na področju obrambe in varstva pred naravnimi in drugimi nesrečami, policija na področju zagotavljanja kibernetske varnosti v okviru javne varnosti in zatiranja kibernetskega kriminala, SOVA na področju protiobveščevalnega delovanja in nastajajoči SIGOV-CERT na področju javne uprave.

Cilji Strategije kibernetske varnosti in ukrepi, potrebni za njihovo doseganje, so navedeni v Tabeli 3.

Tabela 3: Cilji in ukrepi Strategije kibernetske varnosti.

CILJI	UKREPI
1. Okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti	• vzpostavitev osrednje koordinacije nacionalnega sistema zagotavljanja kibernetske varnosti; • kadrovska in tehnološka okrepitev organov na operativni ravni sistema zagotavljanja kibernetske varnosti skupaj z vzpostavitvijo SIGOV-CERT; • redna udeležba na mednarodnih vajah s področja kibernetske varnosti ter izvedba nacionalnih vaj; • postopna nadgradnja omrežja državnih organov HKOM z opremo, ki je ustrezno potrjena s strani slovenskih organov kot varna in primerna za uporabo; • vzpostavitev kompetentnega preverjanja varnosti in funkcionalnosti informacijske opreme v okviru obstoječih in na novo vzpostavljenih organov.
2. Varnost državljanov v kibernetskem prostoru	• redno izvajanje programov ozaveščanja na področju kibernetske varnosti; • uvedba vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja.
3. Kibernetska varnost v gospodarstvu	• spodbujanje razvoja in vpeljave novih tehnologij na področju kibernetske varnosti; • redno izvajanje programov ozaveščanja na področju kibernetske varnosti za gospodarske subjekte.
4. Zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore	• redno ocenjevanje tveganj za delovanje kritične infrastrukture sektorja informacijsko-komunikacijske podpore, načrtovanje ustreznih ukrepov za zaščito ter posodabljanje ocene tveganj na tem področju.
5. Zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala	• implementacija ustreznih kibernetskih zmogljivosti za varovanje informacijskih in komunikacijskih sistemov policije;

CILJI	UKREPI
	• redno usposabljanje s področja kibernetske varnosti za organe pregona, ki sodelujejo pri razvoju kibernetskih zmogljivosti za področje javne varnosti in pri zatiranju kibernetskega kriminala; • redno posodabljanje zakonodaje in postopkov skladno z razvojem informacijsko-komunikacijskih tehnologij.
6. Razvoj obrambnih kibernetskih zmogljivosti	• razvoj ustreznih kibernetskih zmogljivosti za varovanje obrambnih komunikacijskih in informacijskih sistemov.
7. Zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah	• zagotovitev pogojev za nemoteno delovanje ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah.
8. Krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem	• zagotovitev pogojev za sodelovanje slovenskih strokovnjakov v relevantnih mednarodnih delovnih telesih in združenjih s področja kibernetske varnosti.

Vir: Strategija kibernetske varnosti 2015.

5.5.3 Zakonodaja RS, ki se nanaša na informacijsko varnost

Splošna kazniva dejanja, storjena s pomočjo informacijskih tehnologij ali brez njih, so že opredeljena v določilih kaznivih dejanj (npr. kraja, izsiljevanje, povzročanje škode itd.) pri čemer Kazenski zakonik [25] opredeljuje tudi nekatera kazniva dejanja, povezana z informacijskimi sistemi, kot so napad na informacijski sistem, vdori v poslovni informacijski sistem, zloraba osebnih podatkov, izdelovanje pripomočkov za vdor ali neupravičen vstop v informacijski sistem. Ostali zakoni s področja informacijske varnosti so:

- Zakon o elektronskih komunikacijah (ZEKom) [43], ki opredeljuje dolžnosti operaterjev, ki zagotavljajo delovanje komunikacijskih omrežij.
- Zakon o elektronskem poslovanju na trgu (ZEPT) [42], ki ureja način in obseg elektronskega poslovanja na trgu ter opredeljuje odgovornost ponudnika storitve ali gostitelja za podatke, ki so dostopni preko omrežja.
- Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) [41], ki ureja elektronsko poslovanje in uporabo elektronskega podpisa v pravnem prometu, vključujoč tudi elektronsko poslovanje v sodnih, upravnih in drugih podobnih postopkih. Prav tako zakon ureja enakovrednost elektronskega in lastnoročnega podpisa na dokumentih.

Pregled ostalih obstoječih pravnih in drugih podlag, ki se nanašajo na kibernetsko varnost, je razviden iz Priloge 1.

6 Identifikacija in merjenje kibernetskega tveganja

Kibernetsko tveganje dandanes ni več nekaj nepoznanega in neraziskanega. V poplavi vseh metodologij, standardov, protivirusnih programov in pristopov, ki jih predpisujejo in predlagajo najrazličnejše javne in zasebne organizacije, se je pojavila potreba po sistematizaciji pristopov pri ocenjevanju kibernetskega tveganja. Ocenjevanja oziroma merjenja tveganj se lahko lotimo, ko smo tveganja dobro identificirali in opredelili. Ko jih uspemo izmeriti oziroma oceniti, lahko začnemo tveganja spremljati, upravljati in zmanjševati. Določeno poenotenje pristopov je nujno zaradi primerljivosti in spremljanja trendov. V tem poglavju so predstavljeni primeri sistemov ali okvirov za merjenje kibernetskega tveganja, ki so bili razviti ali se razvijajo v zadnjih letih v EU in ZDA.. Samo merjenje tako kompleksnega tveganja, kot je kibernetsko tveganje, je zapleten izziv, saj pogosto nimamo učinkovitih metrik za merjenje posameznih vrst tveganj ali incidentov. Sama analiza preteklih incidentov ne pove dovolj za oceno tveganja, ki so mu organizacije izpostavljene v tem trenutku oziroma v prihodnosti. Ker bi zanašanje na merjenje oziroma na modele, ki bi bili osnovani zgolj na kvantitativnih podatkih, samo po sebi povzročalo večje modelsko tveganje, je potrebna kombinacija vsebinske ocene tveganja, ki je nujno vsaj do določene mere subjektivna, in pa kvantitativne meritve. Da bi bil pristop v čim večji meri konsistenten, okviri in orodja za merjenje kibernetskega tveganja poskušajo v čim večji meri poenotiti vsebinsko odločanje o stopnji tveganja in v čim večji meri definirati kvantitativne kazalnike oz. metrike za merjenja tveganj. Trenutno obstajajo različni okviri in orodja za merjenje in upravljanje kibernetskih tveganj. V nadaljevanju bo predstavljen okvir, ki so ga razvili v Nacionalnem inštitutu za standarde in tehnologijo (ang. *National Institute of Standards and Technology, NIST*) in orodje, ki so ga razvili v Zveznem svetu za nadzor finančnih institucij (ang. *Federal Financial Istitutions Examination Council, FFIEC*) iz ZDA ter pristopi in aktivnosti agencije ENISA, ki izvaja politiko in zakonodajo Evropske unije o zadevah v povezavi z omrežno in informacijsko varnostjo.

6.1 Okvir za izboljšanje kibernetske varnosti kritične infrastrukture

Okvir za izboljšanje kibernetske varnosti kritične infrastrukture (ang. *Framework for Improving Critical Infrastructure Cybersecurity*) Nacionalnega inštituta za standarde in tehnologijo (NIST) iz ZDA, v nadaljevanju okvir NIST, je bil izdan 12. februarja 2014.

Podlaga za izdelavo okvira NIST je s strani predsednika ZDA Baracka Obame izdana odredba (*Executive Order*) 13636 (EO) z dne 12. 2. 2013 z naslovom »Izboljšanje kibernetske varnosti kritične infrastrukture« [19]. Namen odredbe je krepiti odpornost kritične infrastrukture, na kateri temelji nacionalna in gospodarska varnost ZDA. Ta izvršna odredba poziva k razvoju prostovoljnega okvira za kibernetsko varnost, ki zagotavlja prioriteten, prožen in ponovljiv pristop, ki je stroškovno učinkovit in temelji na uspešnosti in s katerim bo možno obvladovati

tveganja, povezana s kibernetsko varnostjo pri postopkih, informacijah in sistemih, ki so neposredno povezani z zagotavljanjem storitev kritične infrastrukture. Okvir NIST, ki je bil razvit v sodelovanju z industrijo, usmerja organizacije pri obvladovanju varnostnih tveganj v kibernetskem prostoru.

Odredba opredeljuje kritično infrastrukturo, fizično in virtualno, ki je ključnega pomena in katere nezmožnost ali uničenje bi katastrofalno vplivalo na varnost, nacionalno gospodarsko varnost, nacionalno javno zdravje oziroma katero koli kombinacijo le teh. Zaradi vedno večjih pritiskov zunanjih in notranjih groženj morajo organizacije, ki so odgovorne za kritično infrastrukturo, z doslednim in ponavljajočim postopkom določiti, oceniti in obvladovati varnostna tveganja v kibernetskem prostoru. Ta pristop zajema javne in zasebne lastnike ter operaterje in druge subjekte, ki so pomembni za varnost državne infrastrukture ne glede na velikost organizacije, njeno izpostavljenost grožnjam ali trenutno izpopolnjenost njene kibernetske varnosti.

Ob priznavanju vloge, ki jo ima varstvo zasebnosti in državljanskih svoboščin pri doseganju večjega zaupanja javnosti, odredba zahteva, da se v okvir NIST vključi metodologijo za zaščito posameznikove zasebnosti in državljanskih svoboščin v primerih, ko organizacije, zadolžene za kritično infrastrukturo, izvajajo aktivnosti, povezane s kibernetsko varnostjo. Metodologija je zamišljena kot dopolnilo teh postopkov in nudi smernice, ki bodo olajšale obvladovanje tveganja kršenja zasebnosti skladno s pristopom, ki ga ima organizacija pri obvladovanju varnostnih tveganj v kibernetskem prostoru.

Da bi bila zagotovljena razširljivost in omogočene tehnične inovacije, je okvir NIST tehnološko nevtralen. Sloni na različnih obstoječih standardih, smernicah in praksah, s katerimi ponudnikom kritične infrastrukture omogoča izboljšanje odpornosti. Razviti okvir NIST je sad skupnega prizadevanja med javnimi organi v ZDA in industrijo ter daje napotke organizacijam pri upravljanju kibernetskega tveganja. Okvir NIST omogoča organizacijam (ne glede na velikost, izpostavljenost kibernetskemu tveganju in trenutne kibernetske grožnje) uporabljati načela in najboljše prakse upravljanja s tveganji za izboljšanje varnosti in odpornosti kritične infrastrukture.

Sam okvir NIST ni vezan na določeno industrijo, prav tako tudi skupna taksonomija standardov, smernic in praks, ki jih zagotavlja, ni vezana na določeno državo. Okvir NIST je primeren za krepitev kibernetske varnosti tudi za organizacije izven ZDA. Okvir NIST lahko prispeva k razvoju skupnega mednarodnega pristopa pri zagotavljanju kibernetske varnosti pri kritični infrastrukturi.

Okvir NIST je na oceni tveganj utemeljen pristop za obvladovanje kibernetskega tveganja in je sestavljen iz treh delov: jedra okvira, izvedbenih nivojev okvira in profila okvira.

Jedro okvira je nabor aktivnosti za izvajanje kibernetske varnosti, želenih rezultatov in ustreznih referenc, ki so skupne kritičnim infrastrukturnim sektorjem. Jedro predstavlja industrijske standarde, smernice in prakse na način, ki omogoča obveščanje o aktivnostih za izvajanje kibernetske varnosti na ravni celotne organizacije, od izvršne do operativne/izvedbene ravni. Jedro okvira tvori pet sočasnih in stalnih funkcij, in sicer:

identifikacija, zaščita, zaznavanje, odzivanje in okrevanje. Če upoštevamo vse funkcije skupaj, dobimo strateški pogled na cikel aktivnosti, povezanih z upravljanjem kibernetskega tveganja oziroma z varnostjo. Vsaka funkcija okvira je nadalje razdeljena na ključne kategorije in podkategorije, ki se neposredno sklicujejo na obstoječe standarde, smernice in prakse.

Izvedbeni nivoji okvira dajejo vsebinsko oceno temu, kako organizacija obravnava kibernetska tveganja in kakšni so vzpostavljeni procesi za obvladovanje teh tveganj. Nivoji določajo, v kolikšni meri se aktivnosti iz jedra okvira (funkcije, kategorije in podkategorije) dejansko izvajajo. Aktivnosti so ovrednotene z enim od štirih nivojev, in sicer od delnega izvajanja (nivo 1) do naprednega izvajanja (nivo 4). Med postopkom izbire nivoja mora organizacija upoštevati svojo trenutno prakso obvladovanja tveganj, zunanje nevarnosti, zakonske zahteve, poslovne cilje/poslanstvo in organizacijske omejitve.

Profil okvira predstavlja rezultate kombinacij med oceno izvedbenih nivojev (ocena nivoja za kategorijo, podkategorijo) in jedrom okvira (kategorije, podkategorije). Profil nato omogoča prepoznavanje slabosti kibernetske varnosti, in sicer s primerjavo »sedanjega« profila (stanje »kot je«) s »ciljnim« profilom (stanje »kakršno naj bo«). Pri oblikovanju profila lahko organizacija pregleda vse kategorije in podkategorije ter na podlagi poslovnega modela in ocene tveganj določi, katere kategorije in podkategorije so najbolj pomembne ter po potrebi doda svoje kategorije in podkategorije, ki so nujne za obravnavo tveganj organizacije.

.

6.2 Orodje za merjenje kibernetskega tveganja

V tem podpoglavju je predstavljeno orodje za merjenje kibernetskega tveganja, ki so ga razvili v Zveznem svetu za nadzor finančnih institucij (ang. *Federal Financial Istitutions Examination Council, FFIEC*) iz ZDA, v nadaljevanju orodje FFIEC.

Zvezni svet za nadzor finančnih institucij iz ZDA je bil ustanovljen 10. marca 1979 v skladu z Zakonom o regulaciji finančnih institucij. FFIEC je formalno medresorski organ, pooblaščen za predpisovanje enotnih načel, standardov, priporočil in obrazcev za poročanje nadzornim organom na zvezni (državni) ravni z namenom spodbujanja enotnosti pri nadzoru finančnih institucij. FFIEC sestavljajo Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), in Consumer Financial Protection Bureau (CFPB).

Glede na vedno večji in vse bolj izpopolnjen obseg kibernetskih groženj je FFIEC razvil in dne 30. junija 2015 objavil orodje za merjenje kibernetskega tveganja za pomoč institucijam pri opredeljevanju njihovih tveganj in za določitev njihove pripravljenosti pri zagotavljanju kibernetske varnosti. Že v pilotni fazi projekta je sodelovalo več kot 500 institucij. Ocena kibernetskega tveganja institucijam zagotavlja ponovljiv in izmerljiv postopek za merjenje njihove pripravljenosti pri zagotavljanju kibernetske varnosti v daljšem časovnem obdobju. Ocena kibernetskega tveganja vključuje načela o kibernetski varnosti, ki jih predpisuje FFIEC, zakonske smernice in načela, ki jih predpisujejo ostali industrijski standardi, vključno s

konceptom okvira NIST Nacionalnega inštituta za standarde in tehnologijo (NIST).

Orodje je v primerjavi z okvirom NIST konkretnejše, saj je osredotočeno na finančne institucije, zaradi česar omogoča merjenje ne samo na podlagi kontrolnega okolja, pač pa tudi na podlagi dejanske izpostavljenosti institucije kibernetskemu tveganju (inherentno tveganje) ne glede na vzpostavljene kontrolne mehanizme.

Ocena je sestavljena iz dveh delov: iz ocene profila tveganja pri normalnem delovanju institucije (inherentno tveganje) in iz ocene kontrolnih mehanizmov za zagotavljanje kibernetske varnosti.

Ocena kontrolnih mehanizmov

Ocena kontrolnih mehanizmov za zagotavljanje kibernetske varnosti je podobno kot pri okviru NIST segmentirana na pet področij, in sicer na:

- obvladovanje tveganj v kibernetskem prostoru in nadzor,
- informacije o tveganjih in sodelovanje,
- kontrolo na področju kibernetske varnosti,
- obvladovanje odvisnosti od zunanjih virov,
- obvladovanje incidentov in odpornost.

Navedena področja ustrezajo petim funkcijam okvira NIST (identifikacija, zaščita, zaznavanje, odzivanje in okrevanje), ki so prav tako kot funkcije okvira NIST nadalje razdeljena na kategorije in podkategorije. Ocenjevanje osnovnih posameznih elementov in podkategorij je za razliko od izbire enega od štirih izvedbenih nivojev izvajanja kontrol pri okviru NIST ocenjeno z dvostopenjsko diskretno oceno (DA/NE). Dvostopenjskemu diskretnemu ocenjevanju so seveda prilagojena vprašanja, ki jih je bistveno več (494) in so bolj neposredna kot pri okviru NIST, kjer je osnovnih elementov za ocenitev manj (98). Če je pri oceni kontrolnih mehanizmov v primeru okvira NIST eno vprašanje, ki pokriva neko področje in ki ga je potrebno oceniti s štiristopenjsko lestvico, imamo v primeru orodja FFIEC več konkretnih vprašanj z možnostjo odgovora DA ali NE. Nadaljnja razlika je v tem, da so vprašanja povezana s kontrolnim okoljem v primeru orodja FFIEC segmentirana v pet skupin glede na zahtevnost (od osnovnih do inovativnih). Vsaka stopnja zahtevnosti vključuje nabor deklarativnih izjav, ki merijo, kako institucija kontrolira tveganja. Ocenjevanje se začne z osnovno stopnjo (osnovne zahteve) in nadaljuje do najvišje, inovativne stopnje zahtevnosti vzpostavljenih kontrol.

Spodaj so navedene opredelitve za vsako stopnjo zahtevnosti kontrolnih mehanizmov:

- **Osnovna zahtevnost [123 vprašanj]** je opredeljena z minimalnimi zahtevami, ki jih predpisujejo zakoni in predpisi oziroma, ki jih priporočajo nadzorne smernice. Ta stopnja vključuje cilje, usmerjene k skladnosti. Vodstvo je smernice pregledalo in ovrednotilo.
- **Razvijajoča se zahtevnost [113 vprašanj]** je opredeljena z dodatno formalnostjo dokumentiranih postopkov in usmeritev, ki še niso predpisane. Cilji so postavljeni na

podlagi tveganj. Formalno se določi odgovornost za kibernetsko varnost. Poleg zaščite podatkov strank vključuje tudi zaščito informacijskih sistemov.

- **Srednjo zahtevnost [113 vprašanj]** določajo podrobni formalni postopki. Kontrole so potrjene in dosledne. Postopki obvladovanja tveganj in analize so zajeti v poslovne strategije.
- **Napredno zahtevnost [86 vprašanj]** določajo postopki in analitika kibernetske varnosti, ki so vključeni v celotno poslovanje. Večina postopkov obvladovanja tveganja je samodejnih in se nenehno izpopolnjujejo. Odgovornost za odločitve o tveganjih je formalno določena.
- **Inovativno zahtevnost [59 vprašanj]** opredeljuje osredotočenost ljudi, postopkov in tehnologij k inovacijam, s katerimi institucija in industrija obvladujeta tveganja v kibernetskem prostoru. Slednje lahko vključuje razvoj novih kontrol in orodij ali oblikovanje novih skupin za izmenjavo informacij.

Glede na model institucije se izbere želeni profil oziroma potrebna stopnja zahtevnosti kontrolnega okolja za kibernetsko varnost.

Ocena profila tveganja (inherentno tveganje)

Bistven doprinos orodja je ocena profila tveganja pri delovanju institucije ne glede na trenutne kontrolne mehanizme (inherentno tveganje). Orodje na podlagi kvantitativnih podatkov določi profil tveganosti naslednjih komponent:

- tehnologija in povezljivost,
- načini dostavljanja informacij/dostavni kanali,
- spletne, mobilne in tehnološke storitve,
- organizacijske značilnosti,
- zunanje grožnje.

Posamezni elementi omenjenih komponent so ocenjeni s petstopenjsko lestvico (zanemarljivo, majhno, zmerno, večje ter znatno tveganje). Ocena profila tveganja pri delovanju institucije vključuje vrsto, obseg in zapletenost dejavnosti ter grožnje, usmerjene proti instituciji. Kombinacija obeh delov – ocene profila tveganja pri delovanju institucije in kontrolnih mehanizmov za zagotavljanje kibernetske varnosti – nato omogoča celovito oceno tveganja institucije glede na njeno naravo.

6.3 Pristopi in aktivnosti Evropske agencije za varnost omrežij in informacij – ENISA

Agencija ENISA izvaja politiko in zakonodajo Evropske unije o zadevah v povezavi z omrežno in informacijsko varnostjo. Strategija kibernetske varnosti Evropske unije [16] predvideva ustanovitev javno zasebne platforme NISP (*Network Information Security Public-Private Platform, NISP*), ki zasleduje iste cilje kot Strategija kibernetske varnosti Evropske unije in Direktiva o varnosti omrežij in informacij (Direktiva NIS). Pomeni, da spodbuja odpornost omrežij in informacijskih sistemov, ki podpirajo storitve, ki jih zagotavljajo operaterji na trgu in administracija v EU. Platforma NISP pomaga izvajati ukrepe, določene v direktivi NIS in zagotavljati njeno usklajeno uporabo v celotni EU. Platforma NISP upošteva mednarodne standarde in najboljše prakse.

Že na prvem sestanku platforme NISP 17. junija 2013 je bilo odločeno, da se ustanovijo tri medsektorske delovne skupine, med njimi skupina za upravljanje s tveganji (vključno z zagotavljanjem informacij, metrik tveganj in ozaveščanjem). Ostali dve skupini delujeta na področju obveščanja o incidentih (izmenjavi informacij) in na raziskavah in inovacijah.
Cilj delovne skupine za upravljanje s tveganji je bil identificirati najboljše prakse za načrtovanje, izdelavo in vzdrževanje procesa upravljanja kibernetskih tveganj tako za male kot velike organizacije iz privatnega in javnega sektorja, pripraviti smernice za izboljšanje informacijske varnosti in olajšati prevzemanje najboljših praks s strani organizacij. Delovna skupina priporoča uporabo najboljših praks v okviru kibernetske varnosti, ki pomaga organizacijam pri izvajanju dejavnosti in pri upravljanju s tveganji na konsistenten način.

Delovna skupina je identificirala različne prakse upravljanja s kibernetskimi tveganji tako v EU in širše in si prizadeva za prenos znanj. Delovna skupina ni predlagala konkretnega modela ali orodja za upravljanje kibernetskega tveganja, pač pa je pripravila priporočila, ki bi pripomogla k bolj enotnemu pristopu merjenja tveganj. V Prilogi 2 so navedeni standardi in okviri, ki se najpogosteje uporabljajo za merjenje kibernetskega tveganja.

Tudi sicer agencija ENISA na domači spletni strani objavlja reference do najpogosteje uporabljenih metod [13] in orodij [14] za upravljanje in merjenje kibernetskega tveganja, ki jih je proučila. Celoten seznam metod in orodij je razviden iz Priloge 3.

Na tretjem plenarnem sestanku platforme NISP dne 30. 4. 2014 je delovna skupina za upravljanje tveganj predstavila dokument »Najboljše prakse pri upravljanju tveganj (ang. *Risk Management Best Practice*)« [12], v katerem je predstavila priporočila za upravljanje kibernetskih tveganj. Pričakovati je, da bo Evropska komisija podprla prizadevanja delovne skupine oziroma platforme NISP. Aprila 2014 je zgolj delovna skupina za upravljanje tveganj štela 122 članov.

Ugotovitve platforme NISP o obvladovanju tveganj bodo podjetjem in javnim organizacijam pomagale povečati svojo kibernetska odpornost in omogočile učinkovitejše sodelovanje med njimi. Ugotovitve delovne skupine oziroma platforme NISP bodo vključene v pripravo priporočil o kibernetski varnosti, ki jih pripravlja Evropska komisija od leta 2014 v sodelovanju z industrijo in javnim sektorjem.

Priporočila delovne skupine, ki se nanašajo na metode, standarde in okvire pri obvladovanja tveganj, se nanašajo na:

- vzpostavitev ustrezne strukture v organizaciji za učinkovito upravljanje s tveganji,
- vzpostavitev učinkovitega poročanja,
- jasno razmejitev odgovornosti v organizaciji,
- jasno strategijo glede informacijskega tveganja,
- upoštevanje kibernetskega vidika tveganja pri novih projektih,
- okrepitev zavedanja o nevarnostih kibernetskega tveganja na vseh nivojih,
- minimalen paket ukrepov na voljo za zmanjševanje kibernetskega tveganja,
- zagotavljanje osnovnih standardov pri obvladovanju tveganj,
- določitev niza standardov, h katerim je organizacija zavezana oziroma, ki jih namerava spoštovati,
- implementacijo niza kibernetsko varnostnih kontrol,
- jasno določenost in razumevanje ter dovzetnost za tveganje.

Delovna skupina za upravljanje tveganj priporoča organizacijam, da vzpostavijo različne metrike (indikatorje) za merjenje kibernetskega tveganja. Slednje omogočajo organizaciji spremljati, kako se izpostavljenost kibernetskemu tveganju spreminja skozi čas. Prav tako delovna skupina za upravljanje tveganj priporoča, da organizacija redno izvaja preglede upravljanja kibernetskega tveganja, ocene ranljivosti, testov vnašanja, delovanja procesov, in uporabljenih metrik (indikatorjev) ter da ocenjuje verjetnost pojavitev nevarnosti.

Metrike, ki jih platforma NISP priporoča organizacijam, so po predlogu strukturirane v tri skupine glede na pomembnost metrike. Seznam je razviden iz Priloge 4.

24. novembra 2014 je bila v Bruslju pod pokroviteljstvom EU in ZDA organizirana delavnica za kibernetsko varnost z namenom primerjave pristopov pri upravljanje kibernetskega tveganja v EU in v ZDA. Na delavnici so strokovnjaki izmenjali izkušnje in poglede glede pristopov v EU in ZDA. Inštitut NIST je predstavil okvir NIST za merjenje kibernetskega tveganja. Generalni direktorat Evropske komisije za komunikacijska omrežja, vsebine in tehnologijo (ang. *European Commission Directorate General for Communications Networks, Content and Technology, DG CONNECT*) pa je predstavil platformo NISP.

6.4 Usmeritve za upravljanje kibernetskega tveganja v bankah

6.4.1 Smernice za kibernetsko odpornost infrastrukture finančnih trgov

Zaradi pomembnosti varnega elektronskega poslovanja oziroma plačevanja in vse večjega kibernetskega tveganja in njegovih zakonitosti ter motivov v povezavi s kriminalnimi dejanji se v zadnjem času kibernetsko tveganje spremlja oziroma obravnava ločeno v okviru informacijskega tveganja. Junija 2016 sta Odbor za plačila in tržne infrastrukture (ang. *Committee on Payments and Market Infrastructures, CPMI*), ki gostuje pri Banki za mednarodne poravnave (BIS) in odbor Mednarodnega združenja nadzornikov trga vrednostnih papirjev (ang. *International Organization of Securities Commissions, IOSCO*) izdala smernice za kibernetsko odpornost infrastrukture finančnih trgov [3].

V prvi vrsti so smernice namenjene odpornosti infrastrukture finančnih trgov (ang. *financial market infrastructures, FMI*) za sistemsko pomembne plačilne sisteme, centralne depotne družbe (ang. *central securities depositories, CSDs*), sisteme za poravnave vrednostnih papirjev (ang. *securities settlement systems, SSSs*), centralne nasprotne stranke (ang. *central counterparties, CCPs*) in repozitorije sklenjenih poslov (ang. *trade repositories, TRs*) ter regulatorje omenjenih sistemov. Smernice so logično sestavljene iz petih osnovnih kategorij upravljanja kibernetskega tveganja in iz treh poglavitnih komponent, ki jih je potrebno obravnavati v povezavi s kibernetsko odpornostjo. Pet osnovnih kategorij pri upravljanju kibernetskega tveganja je: upravljanje, identifikacija, zaščita, zaznavanje ter odzivanje in okrevanje. Poglavitne komponente pa so testiranje, ozaveščanje ter učenje in razvijanje. Struktura ter organiziranost kategorij in komponent je osnovana na trenutno vodilnih in najbolj uveljavljenih standardih in okvirih na področju informacijske in kibernetske varnosti.

Smernice seveda v ničemer ne nadomeščajo niti ne zmanjšujejo veljavnosti obstoječih standardov ali zakonskih zahtev, katerim so institucije zavezane, pač pa jih dopolnjujejo v celostni obravnavi informacijskih in kibernetskih tveganj.

6.4.2 Priporočila za varnost spletnih plačil

Januarja 2013 je ECB izdala priporočila za varnost spletnih plačil [11]. Dokument vsebuje 14 priporočil za izboljšanje varnosti spletnih plačil. Priporočila je pripravil Evropski forum za varnost plačil malih vrednosti (*European Forum on the Security of Retail Payments, SecuRe Pay*). Forum je bil ustanovljen prostovoljno na pobudo nadzornih organov leta 2011. Cilj priporočil je povečati poznavanje in razumevanje med nadzorniki ponudnikov plačilnih storitev v povezavi z varnostjo elektronskih plačilnih storitev malih vrednosti in z instrumenti, ki jih zagotavljajo države članice Evropske unije in Evropskega gospodarskega prostora.

Priporočila so v treh sklopih:

- Splošno kontrolno in varnostno okolje
- Posebni kontrolni in varnostni ukrepi za spletna plačila
- Ozaveščanje, izobraževanje in obveščanje strank

Priporočila v sklopu »Splošno kontrolno in varnostno okolje« obravnavajo vprašanja v povezavi z upravljanjem, prepoznavanjem in ocenjevanjem tveganj, spremljanjem in poročanjem, nadzorom in zmanjševanjem tveganj ter sledljivostjo. Ponudniki spletnih plačil bi morali kot del svojih postopkov za upravljanje tveganj oceniti primernost svojih notranjih varnostnih ukrepov za primere notranjih in zunanjih scenarijev tveganj.

Priporočila v sklopu »Posebni kontrolni in varnostni ukrepi za spletna plačila« vsebujejo vse korake obdelave plačilne transakcije od dostopa do storitve (podatki o stranki, prijava, možnosti avtentikacije) do odreditve plačila, nadzora in odobritve ter zaščite občutljivih podatkov o plačilu.

Priporočila v sklopu »Ozaveščanje, izobraževanje in obveščanje strank« vključujejo zaščito strank, kaj morajo stranke storiti v primeru neželene zahteve po personaliziranih varnostnih poverilnicah, kako varno uporabljati spletne plačilne storitve in kako lahko stranke preverijo, da se je transakcija začela izvajati ter da je bila izvršena.

6.4.3 Smernice za varnosti spletnih plačil

Decembra 2014 je Evropski bančni organ (EBA) izdal smernice o varnosti spletnih plačil [10], ki v celoti povzemajo priporočila Evropskega foruma za varnost plačil malih vrednosti. Glede na vlogo, ki jo ima organ EBA in težo instrumenta smernic, slednje še dodatno zavezujejo vse pristojne organe in finančne institucije, da jih upoštevajo. Nadzorni organi jih morajo ustrezno vključiti v svoje nadzorniške prakse.

EBA je smernice opredelila kot niz minimalnih zahtev oziroma pričakovanj na področju varnosti spletnih plačil. Smernice ne posegajo v odgovornost ponudnikov plačilnih storitev, da spremljajo in ocenjujejo tveganja, prisotna pri njihovih plačilnih operacijah, razvijajo svoje

lastne podrobne varnostne politike ter zagotavljajo ustrezne varnostne ukrepe, ukrepe ob nepredvidljivih dogodkih, ukrepe za obvladovanje incidentov in ukrepe za neprekinjeno poslovanje, ki so sorazmerni s tveganji pri zagotovljenih plačilnih storitvah.
V nadaljevanju so zgolj poimensko navedena priporočila in sklopi, ki so bili predlagani s strani ECB, EBA in Evropskega foruma za varnost plačil malih vrednosti:

Sklop: SPLOŠNO KONTROLNO IN VARNOSTNO OKOLJE

1. Upravljanje
2. Ocena tveganja
3. Spremljanje incidentov in poročanje o njih
4. Nadzor in zmanjševanje tveganj
5. Sledljivost

Sklop: POSEBNI KONTROLNI IN VARNOSTNI UKREPI ZA SPLETNA PLAČILA

6. Začetna identifikacija stranke, podatki
7. Močna avtentikacija strank
8. Registracija in zagotavljanje orodij za avtentikacijo programske opreme, ki jo dobi stranka
9. Poskusi prijave, iztek postopka, veljavnost avtentikacije
10. Spremljanje transakcije
11. Zaščita občutljivih podatkov o plačilih

Sklop: OZAVEŠČANJE, IZOBRAŽEVANJE IN OBVEŠČANJE STRANK

12. Izobraževanje in obveščanje strank
13. Obvestila, določanje omejitev
14. Dostop strank do informacij o statusu postopka odreditve in izvršitve plačila

7 Zasnova sistema za podporo odločanju pri nadzoru kibernetskega tveganja v bankah

V predhodnem poglavju so predstavljena prizadevanja za razvoj pristopov, ki bi olajšali natančnejše merjenje kibernetskega tveganja. Eden prvih je bil okvir NIST Nacionalnega inštituta za standarde in tehnologijo, ki so ga nato med drugim vzeli kot podlago tudi v FFIEC pri razvoju svojega orodja. Evropska agencija ENISA razen konkretnega predloga metrik, ki naj bi jih vseboval model, ni podrobneje opredelila načina merjenja kibernetskega tveganja. Namesto tega je izdala veliko priporočil, primerov dobrih praks in smernic, na podlagi katerih naj bi potem institucije same razvile svoj model obvladovanja kibernetskega tveganja. Okvir NIST kot tudi priporočila agencije ENISA se nanašajo na splošne institucije, medtem ko je orodje FFIEC konkretnejše, saj je prilagojeno finančnim institucijam in zato lahko orodje bolj konkretizira področje metrik za merjenje inherentnega tveganja finančnih institucij. V tem poglavju je predstavljena konceptualna zasnova sistema za podporo odločanju pri nadzoru kibernetskega tveganja v bankah, ki izhaja iz zgoraj omenjenih uveljavljenih praks v svetu.

V predlaganem sistemu za podporo odločanju pri nadzoru kibernetskega tveganja se ločeno ocenijo osnovni elementi kontrolnih mehanizmov oziroma kontrolnega okolja in osnovni elementi inherentnega tveganja. Za ocenjevanje kontrolnega okolja je vzeta podlaga iz okvira NIST. Za oceno inherentnega tveganja so vzete metrike, ki jih je uporabil FFIEC pri svojem orodju. Na podlagi ocen inherentnega tveganja in kontrolnega okolja, sistem za podporo odločanju oceni skupno tveganje in v primeru povečanega tveganja predlaga ukrepe za zmanjšanje tveganja. S tem sistemu za podporo odločanju omogoča lažje vsebinsko odločanje pri izbiri ukrepov pri nadzoru kibernetskega tveganja v bankah.

Sistem za podporo odločanju pri nadzoru kibernetskega tveganja v bankah zagotavlja enotno podlago za razumevanje, ocenjevanje in izražanje varnostnih tveganj v kibernetskem prostoru tako znotraj banke kot zunaj nje. Uporabi se lahko za določanje prednostnih nalog pri zmanjševanju varnostnih tveganj v kibernetskem prostoru in služi kot orodje za usklajevanje politik, poslovanja in tehnoloških pristopov k obvladovanju teh tveganj. Sistem za podporo odločanju se lahko uporabi za merjenje in nadzorovanje kibernetskega tveganje za več bank, lahko pa se osredotoča na identifikacijo kritičnih področij znotraj ene banke.

7.1 Ocenjevanje inherentnega tveganja

Inherentno tveganje predstavlja izpostavljenost banke kibernetskemu tveganju ne glede na trenutno stanje kontrolnega okolja. Inherentno tveganje banke je ocenjeno preko ocen petih kategorij. Ocene tveganj kategorij upoštevajo vrsto, količino in kompleksnost poslovanja banke in grožnje, usmerjene proti njej. Ocene tveganj kategorij se določijo na podlagi ocen osnovnih

elementov znotraj posameznih kategorij. Ocene tveganj za osnovne elemente se raztezajo od najnižje do najvišje stopnje tveganja na petstopenjski lestvici.

Kategorije za oceno inherentnega tveganja so:

- **Tehnologije in povezljivosti [14 elementov/meritev]:** določene vrste povezljivosti in tehnologij lahko predstavljajo večje inherentno tveganje; odvisno od njihove kompleksnosti in zahtevnosti povezav ter od narave določenih tehnoloških izdelkov ali storitev. Ta kategorija ocenjuje število ponudnikov internetnih storitev (ISP) in povezav s tretjimi osebami, gostovanje sistemov, število nezavarovanih povezav, število brezžičnih dostopov, količino omrežnih naprav, izrabljenih sistemov, obseg storitev v oblaku in uporabo osebnih naprav.

- **Dostavni kanali [3 elementov/meritev]:** različni dostavni kanali za izdelke in storitve lahko predstavljajo povečano inherentno tveganje glede na naravo določenega izdelka ali ponujene storitve. Z večjo raznovrstnostjo in številom dostavnih kanalov se veča tudi inherentno tveganje. Ta kategorija ocenjuje dostopnost izdelkov in storitev prek spletnih in mobilnih dostavnih kanalov ter obseg bankomatskega poslovanja.

- **Spletni/mobilni produkti in tehnološke storitve [14 elementov/meritev]:** različni produkti in tehnološke storitve, ki jih ponujajo banke, lahko predstavljajo povečano inherentno tveganje glede na naravo določenega produkta ali ponujene storitve. Ta kategorija ocenjuje različne plačilne storitve, kot so dolžniške in kreditne kartice, plačila med dvema fizičnima osebama (ang. *peer to peer, P2P*), izvorna avtomatizirana klirinška hiša (ACH), elektronski prenosi sredstev v bančnem poslovanju z občani, prenos plačil do trgovcev, storitve zakladništva, skrbniške storitve, globalna nakazila, korespondenčno bančništvo in dejavnosti trgovcev. Ta kategorija upošteva tudi, ali banka zagotavlja tehnološke storitve drugim organizacijam.

- **Organizacijske značilnosti [7 elementov/meritev]:** ta kategorija ocenjuje organizacijske značilnosti, kot so združitve in pripojitve, število uslužbencev in zunanjih izvajalcev storitev kibernetske varnosti, spremembe pri varnostnem osebju, število uporabnikov s privilegiranim dostopom, spremembe v okolju informacijske tehnologije, lokacije poslovne prisotnosti ter lokacije poslovanja in podatkovnih središč.

- **Zunanje grožnje [1 element/meritev]:** količina in vrsta napadov (poskus napadov ali uspešno izvedeni napadi) vplivata na izpostavljenost ustanove inherentnemu tveganju. Ta kategorija ocenjuje količino in izpopolnjenost napadov, usmerjenih proti banki.

Vsako od petih kategorij se oceni na podlagi ocene tveganja za osnovne elemente znotraj kategorije. Ocenjevanje elementov je kvantitativne narave, njihova ocena pa se določi bolj ali manj avtomatsko, saj temelji na vnaprej definiranih metrikah in mejah, ki razmejujejo stopnje tveganj med sabo. Vseh vprašanj za kvantitativno oceno inherentnega tveganja je 39. Za vsak element znotraj posamezne kategorije je potrebno izbrati najustreznejšo stopnja tveganja.

Element, ki se ocenjuje, se lahko nanaša na aktivnost, storitev, produkt ali grožnjo. V tabeli 4 je primer dveh elementov znotraj kategorije Tehnologije in povezljivosti.

Tabela 4: Primer ocenjevanja elementov inherentnega tveganja.

Tveganje / Elementi	Zanemarljivo	Majhno	Zmerno	Večje	Znatno
Skupno število povezav ponudnikov internetnih storitev (ISP) (vključno s podružničnimi povezavami)	Brez povezav	Majhna kompleksnost (1–20) povezav	Zmerna kompleksnost (21–100) povezav	Večja kompleksnost (101–200) povezav	Znatna kompleksnost (>200) povezav
Nezavarovane zunanje povezave, (število povezav neuporabnikov, npr. protokol za prenos datotek (FTP), Telnet, rlogin)	Brez	Malo primerov nezavarovanih povezav (1–5)	Nekaj primerov nezavarovanih povezav (6–10)	Precej primerov nezavarovanih povezav (11–25)	Znatno število primerov nezavarovanih povezav (>25)

Vir: Cybersecurity Assessment Tool (FFIEC).

Seznam vseh elementov po kategorijah za oceno inherentnega kibernetskega tveganja banke je razviden iz Priloge 5.

Opredelitve stopenj inherentnega tveganja so sledeče:

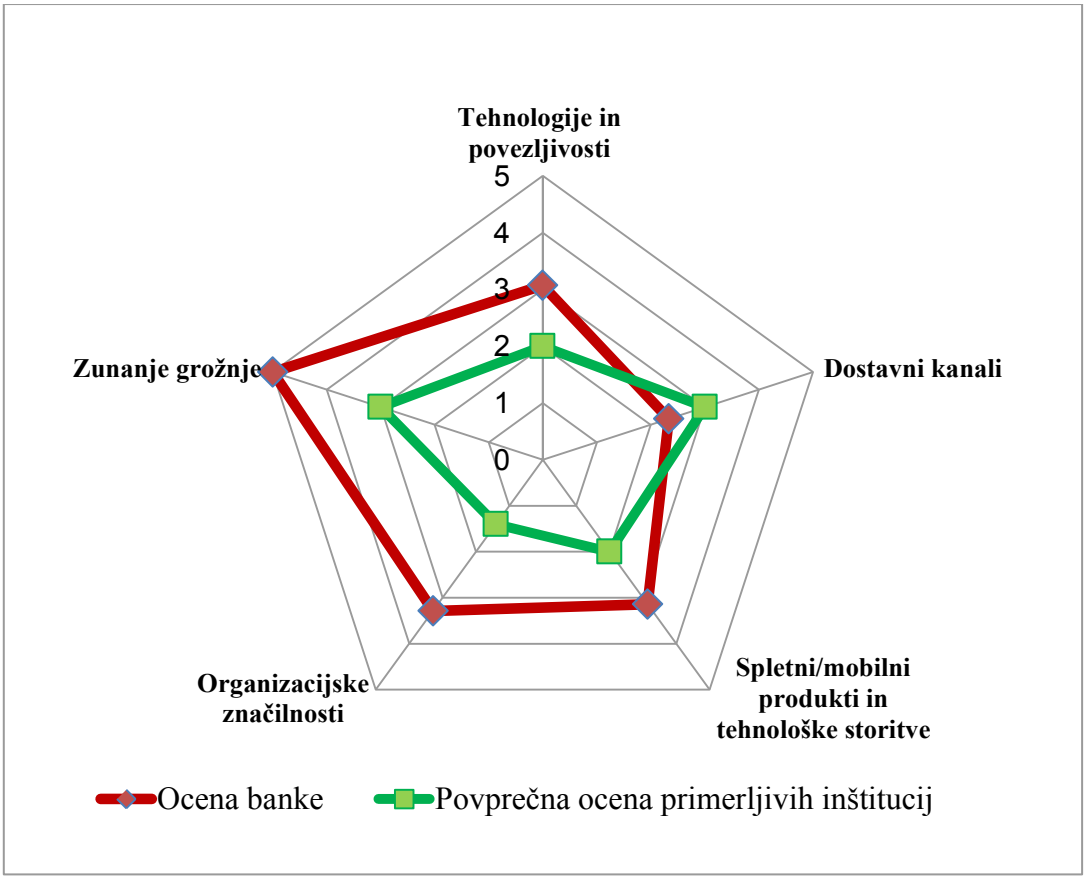
- **Zanemarljivo tveganje.** Na splošno gre za banke z zelo omejeno rabo tehnologije. Takšna banka uporablja malo računalnikov, aplikacij in sistemov ter nobenih povezav. Izbira izdelkov in storitev je omejena. Banka ima majhno regionalno vlogo, malo uslužbencev in običajno ne posluje na drobno.
- **Majhno tveganje.** Banka s profilom majhnega inherentnega tveganja ima omejeno kompleksnost v smislu tehnologije, ki jo uporablja. Ponuja omejeno izbiro manj tveganih produktov in storitev. Sistemi, ki so ključnega pomena, so običajno najeti od zunanjih izvajalcev. Ustanova uporablja predvsem uveljavljene tehnologije. Ima nekaj vrst povezav s strankami in tretjimi osebami z omejeno kompleksnostjo.

- **Zmerno tveganje.** Banka s profilom zmernega inherentnega tveganja na splošno uporablja tehnologijo, ki je lahko kompleksna v smislu količine in izpopolnjenosti. Banka lahko najema sisteme in aplikacije, ki so ključnega pomena za njeno poslanstvo. Njena ponudba izdelkov in storitev je večja in poteka prek različnih kanalov.
- **Večje tveganje.** Banka s profilom večjega inherentnega tveganja na splošno uporablja tehnologijo, ki je kompleksna tako v smislu količine kot tudi izpopolnjenosti. Banka ponuja izdelke in storitve z visokim tveganjem, ki lahko vsebujejo nastajajoče tehnologije. Banka lahko interno gosti precejšnje število aplikacij in omogoča veliko število osebnih naprav ali veliko izbiro vrste naprav. Banka vzdržuje precejšnje število povezav s strankami in tretjimi osebami. Banka ima visok obseg transakcij.
- **Znatno tveganje.** Banka s profilom znatnega inherentnega tveganja uporablja izjemno kompleksne tehnologije za številne izdelke in storitve, ki jih ponuja. Mnogo teh izdelkov in storitev predstavlja najvišjo stopnjo tveganja, vključno s tistimi, ki jih ponuja drugim organizacijam. S številnimi dostavnimi kanali izkorišča nove in nastajajoče tehnologije. Banka lahko najema zunanje izvajalce za sisteme ali aplikacije, ki so ključnega pomena za njeno delovanje. Banka vzdržuje veliko število različnih vrst povezav za prenos podatkov s strankami in tretjimi osebami.

Parametri za določitev inherentnega tveganja niso mišljeni kot togo določeni, temveč so informativno orodje za oceno stopnje tveganja v okviru posamezne aktivnosti, storitve ali produkta. V primerih, kjer je stopnja tveganja ocenjena kot vmesna med dvema stopnjama, se priporoča konservativen pristop oziroma izbira višje stopnje tveganja.

Oceno inherentnega tveganja banke in posameznih kategorij se določi na podlagi ocene elementov. Ocena se lahko izračuna avtomatsko preko pravil združevanja (aritmetična sredina, kvadratična sredina, tehtano povprečje itd.), lahko pa na podlagi ocen elementov, ocenjevalec vsebinsko presodi in oceni kategorijo kot tudi celotno inherentno tveganje banke. Če na primer večina ocen elementov oziroma aktivnosti, produktov ali storitev sodi v zmerno stopnjo tveganja, lahko ocenjevalec oceni, da ima banka zmeren profil inherentnega tveganja. Vendar pa lahko vsaka posamezna kategorija predstavlja drugačno stopnjo tveganja. Zato je lahko končna ocena profila inherentnega tveganja enaka najvišji oceni posamezne kategorije. Zelo pomembno je vzeti v obzir najbolj tvegane ocene posameznih elementov. Če želimo primerjati več bank med seboj ali zasledovati trend ocenjevanja je potrebno združevati ocene posameznih elementov znotraj kategorij in nato primerjati tveganje kategorij. Na sliki 1 je primer grafičnega prikaza tveganosti kategorij inherentnega tveganja.

Slika 1: Grafični prikaz inherentnega tveganja banke.



7.2 Ocenjevanje kontrolnega okolja

Ocenjevanje kontrolnih mehanizmov oziroma kontrolnega okolja za obvladovanje kibernetskega tveganja je razdeljeno v pet funkcij (identifikacija, zaščita, zaznavanje, odzivanje, okrevanje), ki so razdeljene v kategorije in elemente.

Funkcije zagotavljajo aktivnosti za doseganje določenih standardov kibernetske varnosti ter navajajo primere usmeritev za dosego teh ciljev. Funkcije predstavljajo osnovne aktivnosti za izvajanje kibernetske varnosti na najvišji ravni. Banka si z njimi pomaga pri ocenjevanju obvladovanja varnostnih tveganj v kibernetskem prostoru, saj lahko z njihovo pomočjo ureja informacije, omogoča sprejemanje odločitev o obvladovanju tveganj in nevarnosti ter se uči in razvija na podlagi izkušenj iz preteklih aktivnosti. Definicije funkcij so skladne z obstoječimi metodologijami za obvladovanje incidentov in omogočajo prikaz rezultatov vlaganj v kibernetsko varnost.

Kategorije pomenijo razčlenitev funkcije v skupine kibernetske varnosti in so tesno povezane s programskimi potrebami in določenimi aktivnostmi.

Osnovni elementi členijo kategorijo v določene skupine tehničnih oziroma upravljavskih

aktivnosti. Elementi zagotavljajo sklop ocen, ki omogočajo ocenjevanje kontrolnih mehanizmov v posamezni kategoriji. Elemente je potrebno vsebinsko oceniti glede na štiristopenjsko lestvico (se ne izvaja, delno izvajano, v veliki meri izvajano, v celoti izvajano) ustreznosti izvajanja kontrol oziroma aktivnosti. Elementi predstavljajo ključne zahteve za kibernetsko varnost, ki jih je industrija prepoznala kot koristne pri obvladovanju varnostnih tveganj v kibernetskem prostoru. Izhajajo iz uveljavljenih in sprejetih standardov, smernic in praks, ki so skupne ključnim infrastrukturnim sektorjem in ki omogočajo ocenjevanje ustreznosti kontrol, ki so povezane s posamezno kategorijo. V tabeli 5 je prikazana segmentacija kontrolnih mehanizmov na funkcije in kategorije.

Tabela 5: Segmentacija kontrolnih mehanizmov.

Funkcija	Kategorija
Identifikacija	upravljanje sredstev
	poslovno okolje
	upravljanje
	ocena tveganja
	strategija upravljanja s tveganji
Zaščita	nadzor dostopa
	ozaveščanje in usposabljanje
	varnost podatkov
	procesi in postopki za zaščito informacij
	vzdrževanje
	zaščitna tehnologija
Zaznavanje	anomalije in dogodki
	stalni nadzor varnosti
	procesi zaznavanja
Odzivanje	načrtovanje odzivov
	komunikacije
	analiza
	ublažitev posledic
	izboljšave
Okrevanje	načrtovanje okrevanja
	izboljšave
	komunikacije

Vir: Framework for Improving Critical Infrastructure Cybersecurity (NIST).

Celoten seznam vseh funkcij, kategorij, elementov in referenc, na katere se nanašajo elementi, je razviden iz Priloge 6.

V nadaljevanju je natančneje opredeljenih pet funkcij za ocenjevanje kontrolnih mehanizmov kibernetskega tveganja.

- **Identifikacija** – razviti zavedanje organizacije o obstoju kibernetskega tveganja in ga znati identificirati, da se ga nato lahko obvladuje.

  Aktivnosti v funkciji identifikacija so temeljne za učinkovit sistem ocenjevanja kibernetskega tveganja. Razumevanje poslovnega konteksta, virov, ki podpirajo kritične funkcije in povezanih varnostnih kibernetskih tveganj, omogoča organizaciji, da se osredotoča in določi prednostne naloge v skladu s svojo strategijo obvladovanja tveganj in poslovnimi potrebami. Kategorije v tej funkciji so: upravljanje sredstev, poslovno okolje, upravljanje, ocena tveganja in strategija upravljanja s tveganji.

- **Zaščita** – razviti in izvajati ustrezne zaščitne ukrepe za zagotavljanje kritičnih infrastrukturnih storitev.

  Funkcija zaščita omogoča omejevanje oziroma zajezitev vpliva potencialnih kibernetskih groženj. Kategorije v tej funkciji so: nadzor dostopa, ozaveščanje in usposabljanje, varnost podatkov, procesi in postopki za zaščito informacij, vzdrževanje in zaščitna tehnologija.

- **Zaznavanje** – razviti in izvajati ustrezne aktivnosti za prepoznavanje dogodkov, povezanih s kibernetsko varnostjo.

  Funkcija zaznavanje omogoča pravočasno zaznavanje dogodkov, povezanih s kibernetsko varnostjo. Kategorije v tej funkciji so: anomalije in dogodki, stalni nadzor varnosti in procesi odkrivanja.

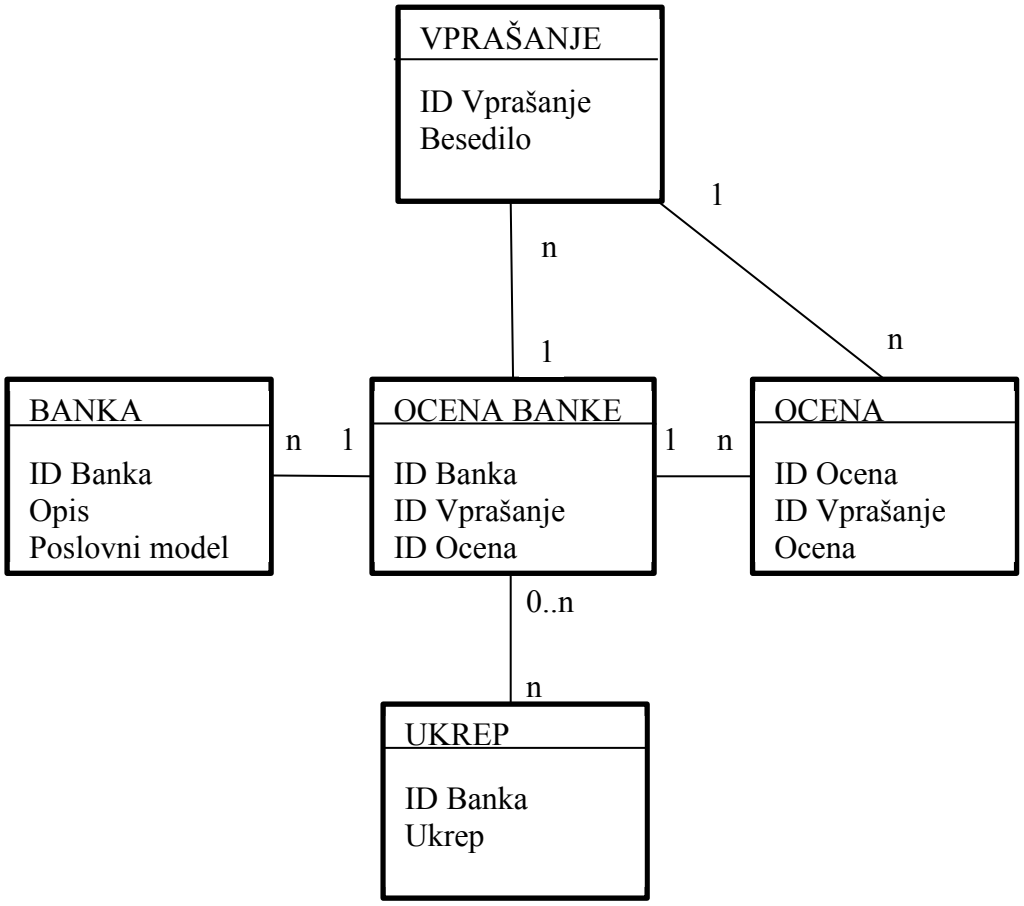
- **Odzivanje** – razviti in izvajati ustrezne aktivnosti za ukrepanje glede odkritih dogodkov, povezanih s kibernetsko varnostjo.
  Funkcija odzivanje omogoča zajezitev vpliva potencialnih kibernetskih dogodkov. Kategorije v tej funkciji so: načrtovanje odzivov, komunikacije, analiza, ublažitev posledic in izboljšave.

- **Okrevanje** – razviti in izvajati ustrezne aktivnosti za načrtovanje odpornosti in obnovo vseh zmogljivosti oziroma storitev, ki so bile okvarjene zaradi dogodka, povezanega s kibernetsko varnostjo.
  Funkcija okrevanje omogoča pravočasno vrnitev k običajnemu poslovanju in zmanjšuje učinke dogodkov, povezanih s kibernetsko varnostjo. Kategorije v tej funkciji so: načrtovanje okrevanja, izboljšave in komunikacije.

7.3 Meta podatkovni model

Na sliki 2 je prikazan poenostavljen meta podatkovni model ter povezave in razmerja med tabelami, v katerih so shranjeni vhodni in izhodni podatki sistema za podporo odločanju pri nadzoru kibernetskega tveganja v bankah.

Slika 2: Meta podatkovni model sistema za podporo odločanju.



8 Aplikacija sistema za podporo odločanju pri nadzoru kibernetskega tveganja v bankah

V predhodnem poglavju je predstavljena konceptualna zasnova in vsebina sistema za podporo odločanju pri nadzoru kibernetskega tveganja v bankah. Določene in opisane so funkcije, kategorije in osnovni elementi (aktivnosti, storitve, produkti, kontrole, zahteve), ki so relevantni na področju kibernetskega tveganja. Predlagan je tudi pristop, ki naj bo uporabljen pri oceni kontrolnih mehanizmov in način merjenja inherentnega tveganja, v kolikor je le mogoče s kvalitativnimi in kvantitativnimi usmeritvami/kriteriji. V tem poglavju je predstavljena aplikacija sistema za podporo odločanju pri nadzoru kibernetskega tveganja, ki omogoča iz ocen in meritev osnovnih elementov transparentno oceniti celotno kibernetsko tveganje banke, identificirati kritična področja v povezavi s kibernetskim tveganjem ter predlagati ukrepe za zmanjšanje tveganja.

Sistem za podporo odločanju lahko uporablja banka z namenom merjenja ter omejevanja kibernetskega tveganja oziroma z namenom okrepitve svoje kibernetske varnosti. Sistem za podporo odločanju lahko služi bančnim nadzornim institucijam, ki na podlagi meritve oziroma informacij, ki so jih pridobili tekom nadzora, ocenijo izpostavljenost nadzorovanih institucij kibernetskemu tveganju. Od vrste ocenjevanja in izbire načina izvedbe merjenja tveganja je potem odvisna tudi implementacija oziroma prilagoditev sistema kot tudi interpretacija rezultatov in nadaljnje aktivnosti.

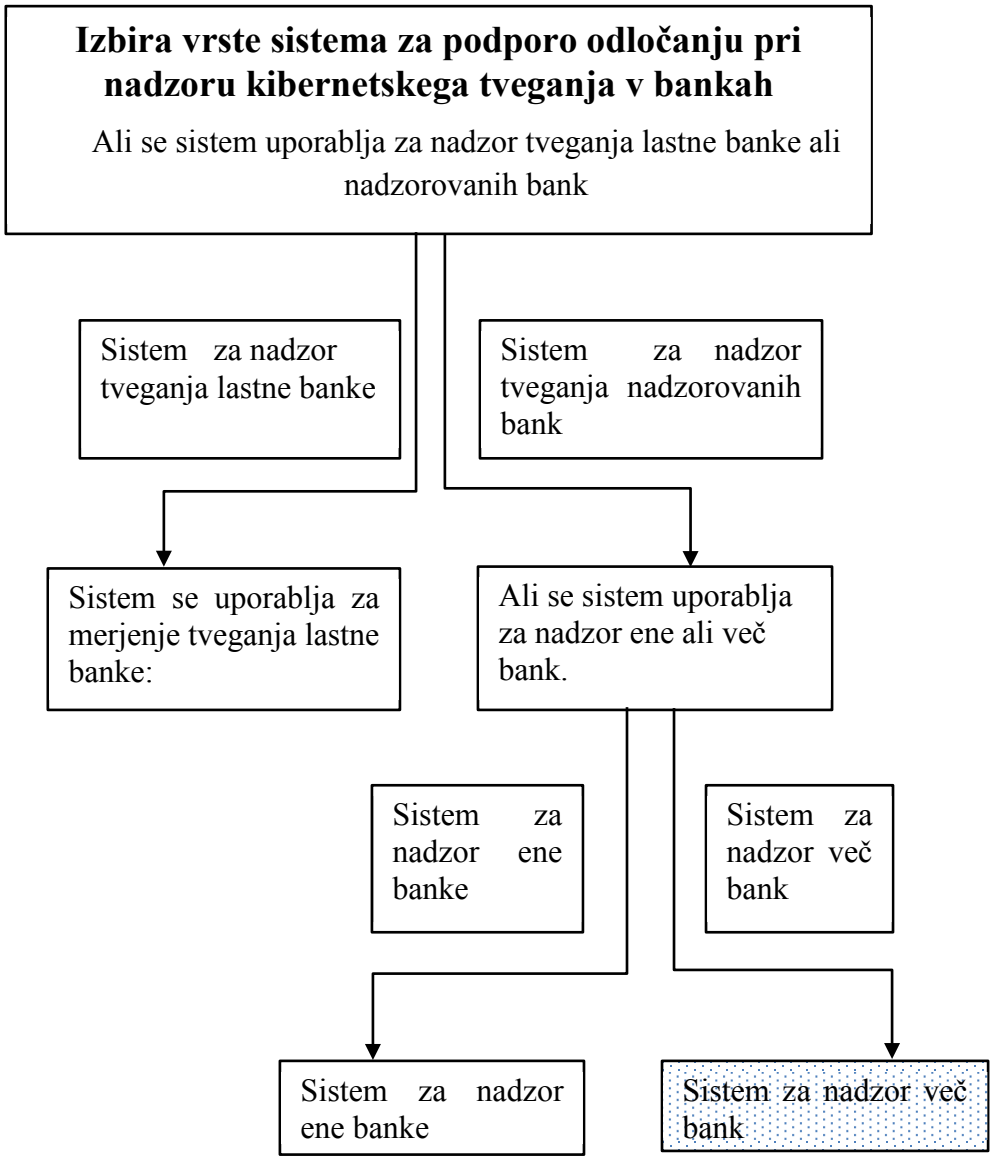
Nadzorna institucija lahko pošlje vprašalnik nadzorovanim bankam z zahtevo, da banka sama izvede samoocenitev (odgovori na vprašanja v povezavi s kontrolnim okoljem in inherentnim tveganjem). V tem primeru lahko ocenjevanje izvede oddelek notranje revizije v banki. Banka lahko najeme zunanjega neodvisnega ocenjevalca, ki izvede ocenjevanje. Takšno ocenjevanje lahko opravijo neodvisne revizorske hiše, ki redno revidirajo poslovanje banke in v bankah preživijo večino delovnega časa. V kolikor je namen izmeriti tveganje ene same nadzorovane banke, si nadzorna institucija lahko privošči, da napoti v nadzorovano banko svoje strokovnjake, ki izvedejo ocenjevanje. V kolikor se želi izmeriti tveganje v nekaj sto ali tisoč bankah, običajno izvedbo oziroma organizacijo ocenjevanja zagotovijo banke same. V takšnem primeru se od bank zahteva, da posredujejo tudi ustrezno dokumentacijo oziroma dokazila, ki potrjujejo pravilnost ocene in ocenjevanja. Pri samoocenjevanju je potrebno upoštevati, da je pristop pri ocenitvi bolj mehkih dejavnikov pogosto premalo konservativen in je morda potrebna določena prilagoditev rezultatov merjenja. Primera takšnih vprašanj za oceno kontrolnih mehanizmov sta na primer vprašanji: »Ali se ugotovijo odvisnosti in funkcije za zagotavljanje ključnih storitev?« in »Ali je vzpostavljena informacijska varnostna politika?« Pri ocenjevanju je potrebno izbrati najbolj ustrezno stopnjo izvajanja med štirimi možnostmi (se ne izvaja, delno izvajano, v veliki meri izvajano, v celoti izvajano). Pri oceni inherentnega tveganja je mehkih dejavnikov nekoliko manj, vendar se pogosto pojavi vprašanje pravilne interpretacije vprašanja. Primer je element (vprašanje), ki ocenjuje inherentno tveganje (kategorija: Organizacijske značilnosti), in sicer stopnjo spremembe v IT okolju (npr. omrežje, infrastruktura, ključne aplikacije, podporne tehnologije za nove izdelke ali storitve), na izbiro

pri ocenjevanju pa je naslednjih pet možnosti: stabilno IT okolje, redke ali minimalne spremembe v IT okolju, redno sprejemanje novih tehnologij, velik obseg večjih sprememb, pogoste obsežne in kompleksne spremembe v okolju.

Sistem za podporo odločanju, predstavljen v magistrskem delu, je zasnovan za nadzor kibernetskega tveganja poljubnega števila bank (npr. več tisoč). Ena glavnih lastnosti takšnega sistema je sposobnost združevanja in ovrednotenja ogromnega števila ocen osnovnih elementov inherentnega tveganja in kontrolnega okolja v vsebinsko obvladljive skupine po kategorijah, funkcijah in drugih segmentih.

Na sliki 3 je modul, ki predstavlja odločitveni sistem za podporo odločanju o tem, katera vrsta sistema za podporo odločanju pri nadzoru kibernetskega tveganja v bankah je najbolj primerna glede na želen način nadzora/ocenjevanja nadzorovanega subjekta.

Slika 3: Izbira vrste sistema za podporo odločanju.



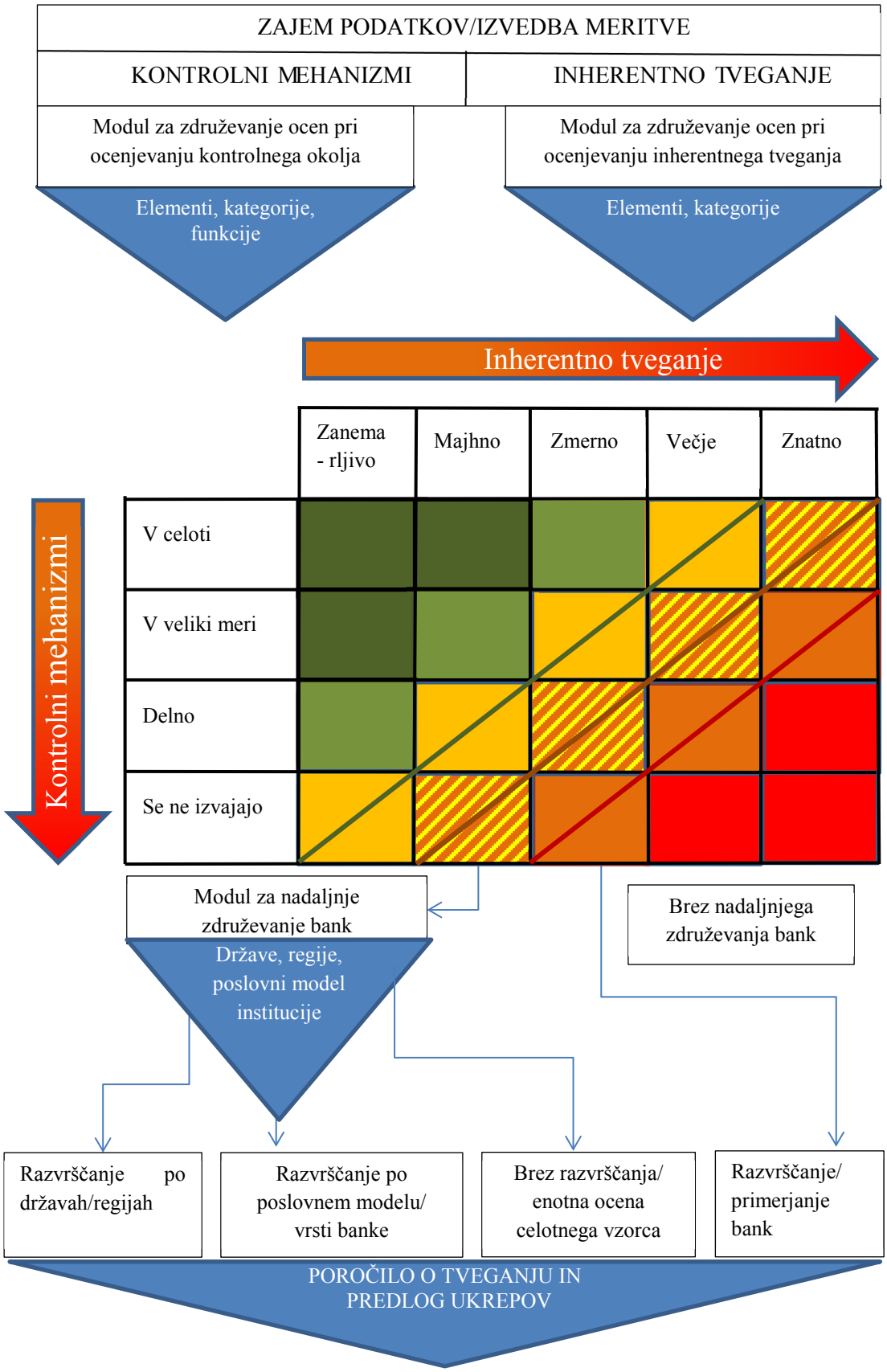
Ključni izziv pri izdelavi sistema za podporo odločanju pri nadzoru kibernetskega tveganja v bankah je zagotoviti njegovo sposobnost identifikacije kritičnih področij kibernetskega tveganja. Tako je pomembna identifikacija najbolj kritičnih bank, najbolj kritičnih funkcij, kategorij in elementov pri kontrolnem okolju in inherentnem tveganju po različnih segmentih. Segmenti, za katere nas zanima izpostavljenost kibernetskemu tveganju, so najpogosteje države, regije in poslovni modeli/vrste bank.

Ko je določen vzorec bank, na katerih bo izvedena meritev kibernetskega tveganja in način ocenjevanja osnovnih elementov tveganja (samoocenitev, ekspertne ekipe, zunanji neodvisni ocenjevalci), se temu lahko prilagodijo osnovni elementi kontrolnih mehanizmov in inherentnega tveganja, ki so predmet ocenjevanja skupaj z usmeritvami ali mejami v primeru kvantitativnih vprašanj. Glede na izbiro vzorca se lahko pojavi potreba po dodajanju novih osnovnih elementih, ki jih je potrebno oceniti oziroma potreba po prilagoditvi obstoječih.

Na sliki 4 je prikazana arhitektura aplikacije odločitvenega sistema za nadzor kibernetskega tveganja v banki, ki je sestavljena iz naslednjih logičnih enot:

- Zajem podatkov/izvedba meritve.
- Modul za združevanje ocen pri ocenjevanju kontrolnega okolja.
- Modul za združevanje ocen pri ocenjevanju inherentnega tveganja.
- Združevanje oceni kontrolnega okolja in inherentnega tveganja.
- Modul za nadaljnje združevanje bank po segmentih.
- Razvrščanje in identifikacija.
- Poročilo o tveganju in predlog ukrepov.

Slika 4: Arhitektura sistema za podporo odločanju.



V naslednjih podpoglavjih so podrobno razložene vse logične enote.

8.1 Zajem podatkov/izvedba meritve

Zajem podatkov/izvedba meritve zagotavlja vhodne podatke, ki jih sistem za podporo odločanju obdela in na podlagi katerih se predlagajo ukrepi in sprejemajo odločitve. Ko je določena konceptualna zasnova, izbrana vrsta sistema in definirana vsebina, to so: osnovni elementi (vprašanja), metrike in kriteriji (usmeritve) pri ocenjevanju, nadaljnje procesiranje poteka precej avtomatizirano. V primeru sistema za podporo odločanju pri nadzoru kibernetskega tveganja v bankah, ki je predstavljen v magistrskem delu, gre za oceno 89 elementov (vprašanj) s področja izvajanja kontrolnih mehanizmov z možnimi odgovori (1 – v celoti, 2 – v veliki meri, 3 – delno, 4 – se ne izvajajo) in 39 ocen elementov inherentnega tveganja z možnimi odgovori (1 – zanemarljivo, 2 – majhno, 3 – zmerno, 4 – večje, 5 – znatno). Uporabniški vmesnik za vnos podatkov v aplikacijo je lahko spletna stran, predloga v Excelu ali vprašalnik.

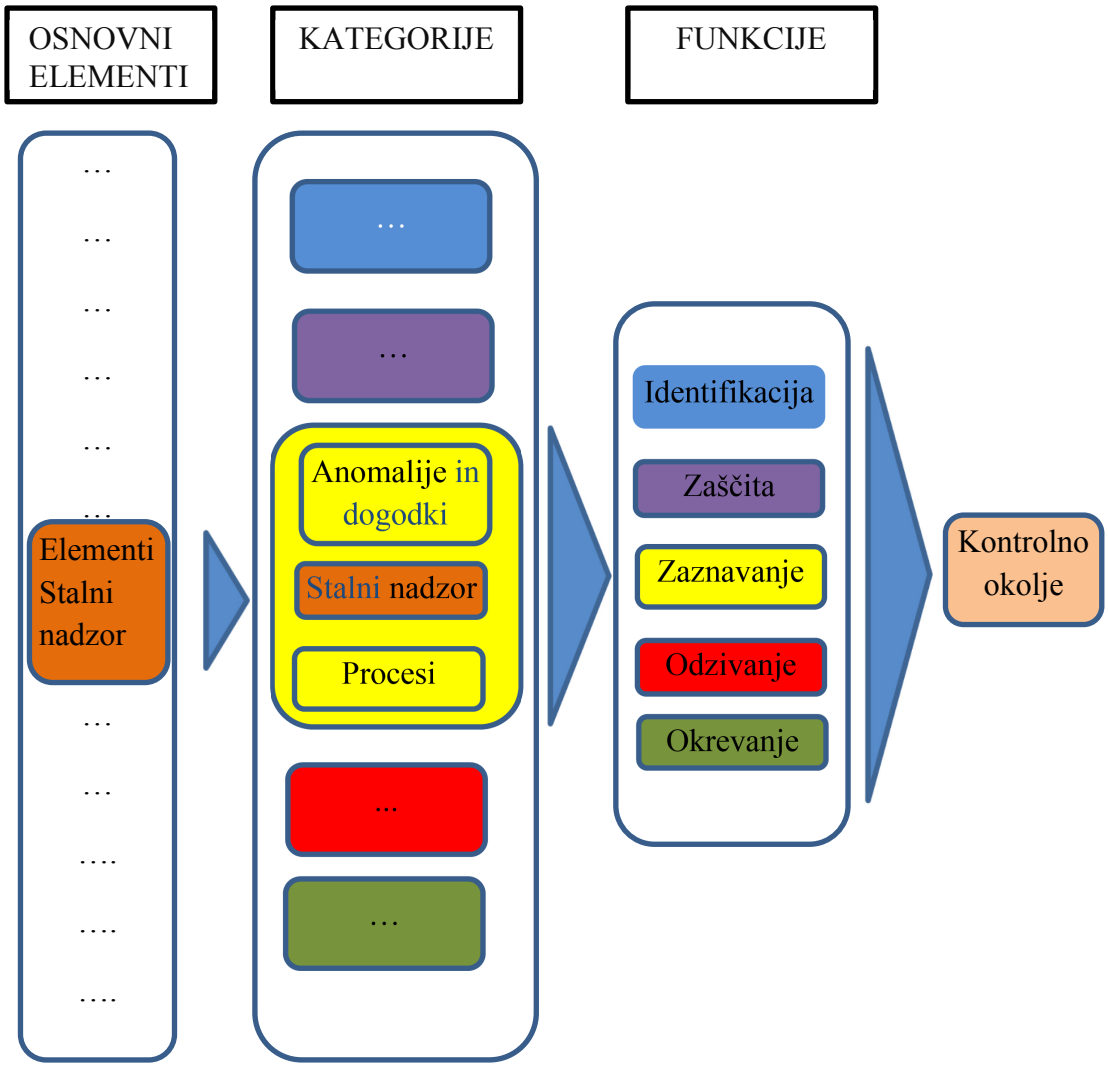
8.2 Modul za združevanje ocen pri ocenjevanju kontrolnega okolja

Naloga modula za združevanje ocen pri ocenjevanju kontrolnega okolja je iz 98 ocen posameznih osnovnih elementov le-te strniti v enotno oceno, ki bo pravilno odražala oceno kontrolnega okolja banke. Ocena kontrolnega okolja v numerični obliki se nahaja znotraj intervala [1–4], kar ustreza 4-stopenjski lestvici za oceno osnovnih elementov (1 – v celoti, 2 – v veliki meri, 3 – delno, 4 –se ne izvajajo). Pri združevanju je potrebno zasledovati zakonitosti in strukturo kontrolnih mehanizmov. Zgolj seštevanje in računanje povprečja ocen posameznih elementov ni na mestu, saj smo v primeru izvajanja kontrolnih mehanizmov v veliki meri izpostavljeni povečanemu tveganju, če je delovanje zgolj ene od funkcij (identifikacija, zaščita, zaznavanje, odzivanje, okrevanje) neustrezno. Ker je odpornost kibernetskega tveganja odvisna od delovanja vseh funkcij, je potrebno v takšnem primeru največji oziroma ves poudarek dati najslabše ocenjeni funkciji pri oceni kontrolnega okolja banke.

Podobno je potrebno pri oceni posamezne funkcije večji poudarek pri združevanju dati slabše ocenjenim kategorijam znotraj funkcije. Pri ocenjevanju posameznih kategorij, ki so nadalje razčlenjene na osnovne elemente, ki so predmet osnovnega ocenjevanja, je poudarek na najslabše ocenjenih elementih nekoliko manj izrazit.

Iz Slike 5, ki prikazuje arhitekturo modula za združevanje ocen pri ocenjevanju kontrolnega okolja, so razvidni postopki združevanja ocen osnovnih elementov v oceno kategorije, nato v oceno funkcije in nato v oceno kontrolnega okolja.

Slika 5: Združevanje ocen pri ocenjevanju kontrolnega okolja.



V modulu potekajo trije nivoji združevanj, in sicer:

- združevanje ocen osnovnih elementov znotraj ene kategorije v oceno kategorije,
- združevanje ocen kategorij znotraj ene funkcije v oceno funkcije,
- združevanje ocen funkcij v oceno kontrolnega okolja.

Za vsako od teh treh združevanj so možni trije načini, in sicer glede na poudarek slabše ocenjenim področjem:

- velik poudarek slabše ocenjenim področjem,
- zmerni poudarek slabše ocenjenim področjem,
- enak poudarek bolje in slabše ocenjenim področjem.

V tabeli 6 so predstavljeni vsi načini združevanja glede na poudarek slabše ocenjenim elementom in nivo združevanja.

Tabela 6: Načini združevanja ocen pri ocenjevanju kontrolnega okolja.

Stopnja združevanja / Vrsta združevanja	Velik poudarek slabše ocenjenim področjem	Zmerni poudarek slabše ocenjenim področjem	Enak poudarek boljše in slabše ocenjenim področjem.
Osnovni elementi → Kategorija	Kvadratična sredina	Kvadratična sredina	Aritmetična sredina
Kategorije → Funkcija	Maksimum	Kvadratična sredina	Aritmetična sredina
Funkcije → Kontrolno okolje	Maksimum	Aritmetična sredina treh najslabše ocenjenih funkcij	Aritmetična sredina

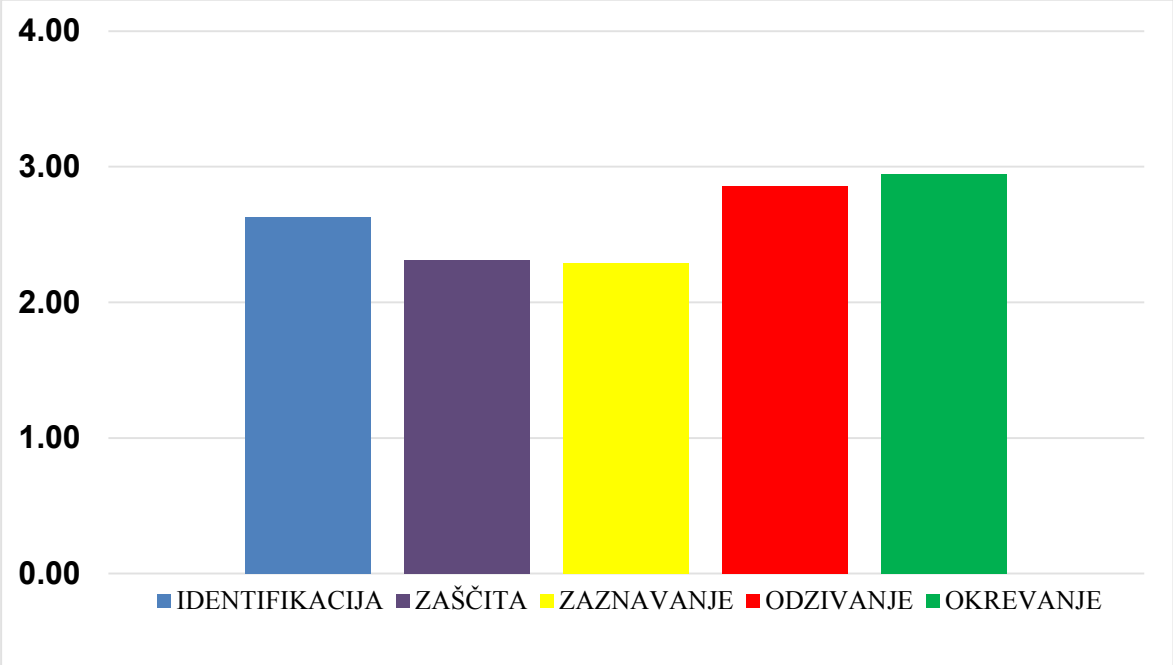
Stopnja poudarka slabše ocenjenim področjem pri združevanju ocen je vhodni parameter v sistem za podporo odločanju, ki ga določi uporabnik sistema za podporo odločanju glede na želeno analizo oziroma interpretacijo rezultatov. V primeru iskanja najbolj kritičnih področij in ekstremnih vrednosti pri bankah je smiselno izbrati način, ki da velik poudarek slabše ocenjenim elementom. V primeru nadaljnjega združevanja bank po segmentih je zaradi predstavljivosti smiselno izbrati stopnjo z enakim poudarkom boljše in slabše ocenjenim elementom. Pri običajni uporabi sistema za odločanje je pri združevanju predvidena izbira stopnje z zmernim poudarkom slabše ocenjenim elementom. Kvadratična sredina je eden od načinov, ki poudari slabše (višje) ocene pri združevanju. V tabeli 7 je prikazan hipotetičen primer ocene kontrolnih mehanizmov po posameznih funkcijah.

Tabela 7: Ocena funkcij in kontrolnega okolja.

Kategorija	Št. elementov	V celoti izvajano 1	V veliki meri izvajano 2	Delno izvajano 3	Ni izvajano 4	Povprečje
IDENTIFIKACIJA	24	2	8	11	3	2,63
ZAŠČITA	35	5	17	9	4	2,31
ZAZNAVANJE	18	1	13	3	1	2,29
ODZIVANJE	15	2	3	9	1	2,86
OKREVANJE	6	0	3	2	1	2,94
Skupaj	98	10	44	34	10	2,61

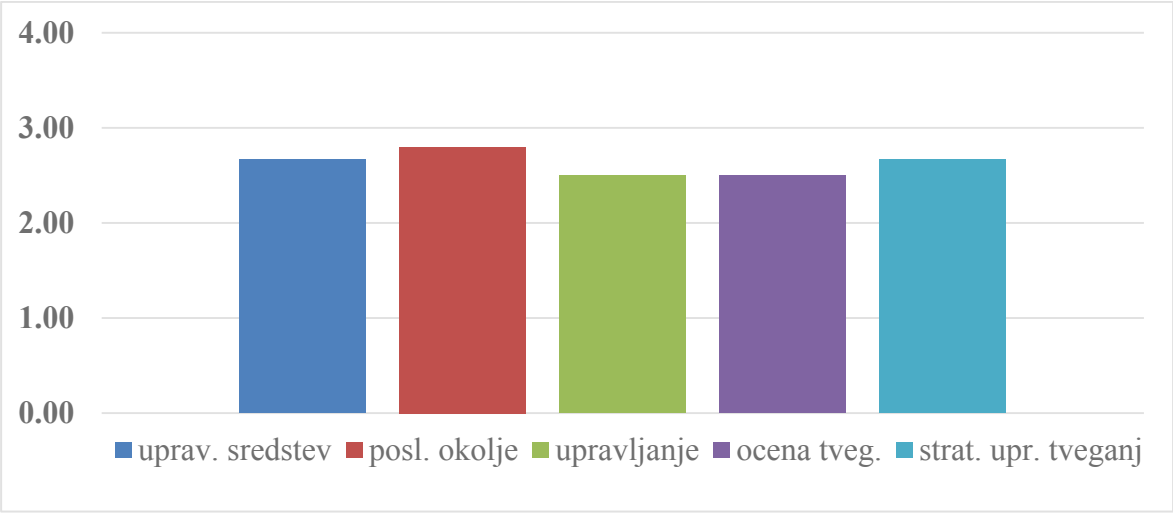
Pri končni oceni kontrolnega okolja je potrebna osredotočenost na najšibkejši člen oziroma funkcijo. Za učinkovito delovanje kontrolnih mehanizmov morajo ustrezno delovati vse funkcije.

Slika 6: Ocene funkcij kontrolnega okolja.



Pri analizi rezultatov lahko posamezno funkcijo nadalje analiziramo glede na ocene posameznih kategorij oziroma elementov. Na sliki 7 je primer ocen kategorij za funkcijo »identifikacija«.

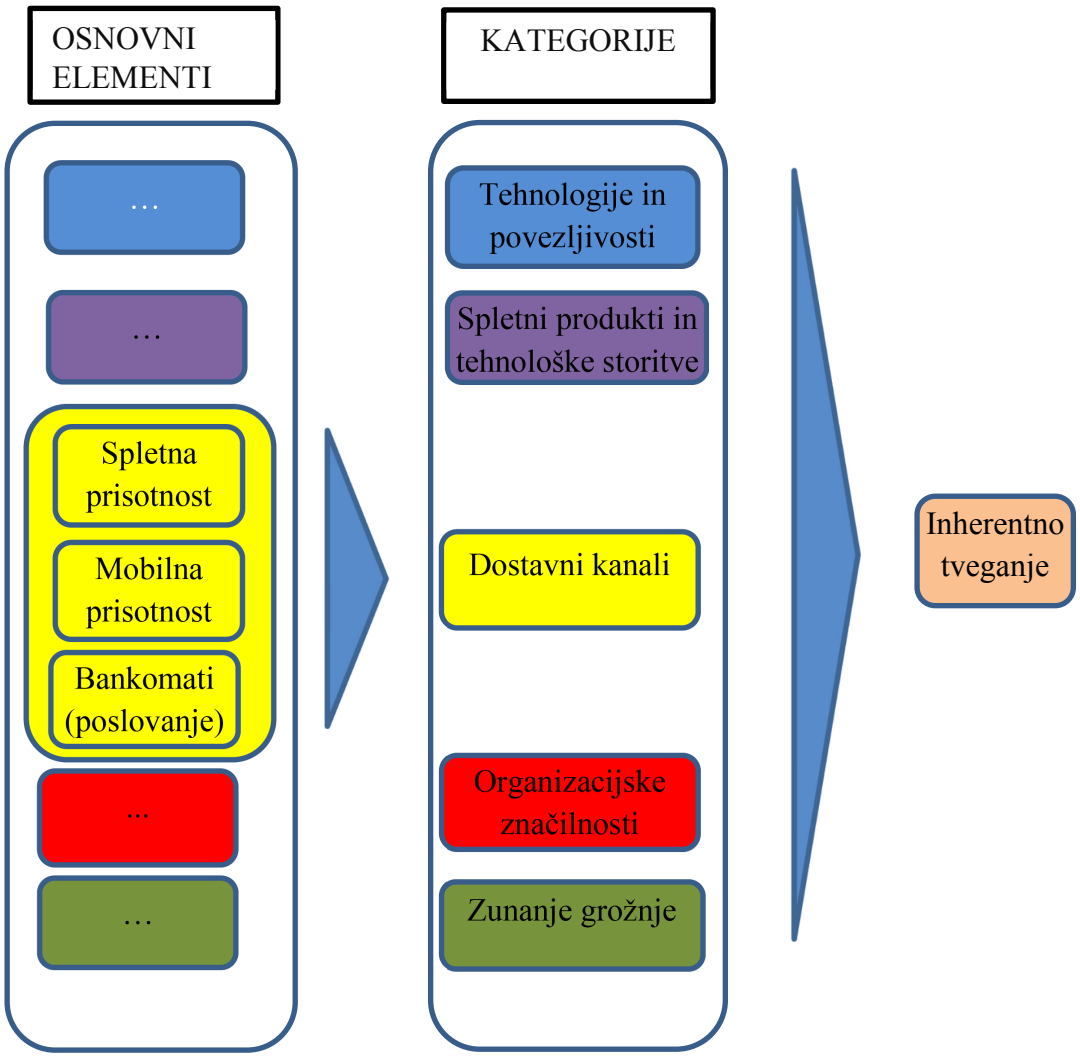
Slika 7: Ocene kategorij funkcije »identifikacija«.



8.3 Modul za združevanje ocen pri ocenjevanju inherentnega tveganja

Naloga modula za združevanje ocen pri ocenjevanju inherentnega tveganja je iz 39 ocen osnovnih elementov (metrik) le-te strniti v enotno oceno, ki bo pravilno odražala skupno oceno inherentnega tveganja banke. Skupna ocena v numerični obliki se nahaja znotraj intervala [1–5], kar ustreza 5-stopenjski lestvici za oceno inherentnega tveganja osnovnih elementov (1 – zanemarljivo do 5 – znatno). Tako kot pri modulu za združevanje ocen pri ocenjevanju kontrolnega okolja je tudi pri modulu za združevanje pri ocenjevanju inherentnega tveganja potrebno pri združevanju zasledovati zakonitosti posameznih kategorij inherentnega tveganja. Tudi pri inherentnem tveganju je v primeru združevanja ocen osnovnih elementov v kategorije in nato v končno oceno inherentnega tveganja poudarek na slabše ocenjenih področjih.
Iz slike 8, ki prikazuje arhitekturo modula za združevanje pri ocenjevanju inherentnega tveganja, so razvidni postopki združevanja ocen osnovnih elementov v oceno kategorije in nato v oceno inherentnega tveganja.

Slika 8: Združevanje ocen pri ocenjevanju inherentnega tveganja.



V modulu potekata dva nivoja združevanj, in sicer:

- Združevanje ocene osnovnih elementov znotraj ene kategorije v oceno kategorije.
- Združevanje ocen kategorij v oceno inherentnega tveganja.

Za vsako od obeh združevanj so možni trije načini, in sicer glede na poudarek slabše ocenjenim področjem:

- velik poudarek slabše ocenjenim področjem,
- zmerni poudarek slabše ocenjenim področjem,
- enak poudarek bolje in slabše ocenjenim področjem.

V tabeli 8 so predstavljeni vsi načini združevanja glede na poudarek slabše ocenjenim področjem in nivo združevanja.

Tabela 8: Načini združevanja ocen pri ocenjevanju inherentnega tveganja.

Stopnja združevanja / Vrsta združevanja	Velik poudarek slabše ocenjenim področjem	Zmerni poudarek slabše ocenjenim področjem	Enak poudarek bolje in slabše ocenjenim področjem.
Osnovni elementi → Kategorija	Kvadratična sredina	Kvadratična sredina	Aritmetična sredina
Kategorije → Inherentno tveganje	Maksimum	Kvadratična sredina	Aritmetična sredina

Izbira stopnje poudarka slabše ocenjenim področjem zasleduje pri združevanju ocen elementov v oceno inherentnega tveganja banke isto logiko kot pri združevanju ocen elementov pri kontrolnem okolju in je opisana v predhodnem podpoglavju. V tabeli 9 je hipotetičen primer ocene inherentnega tveganja po posameznih kategorijah.

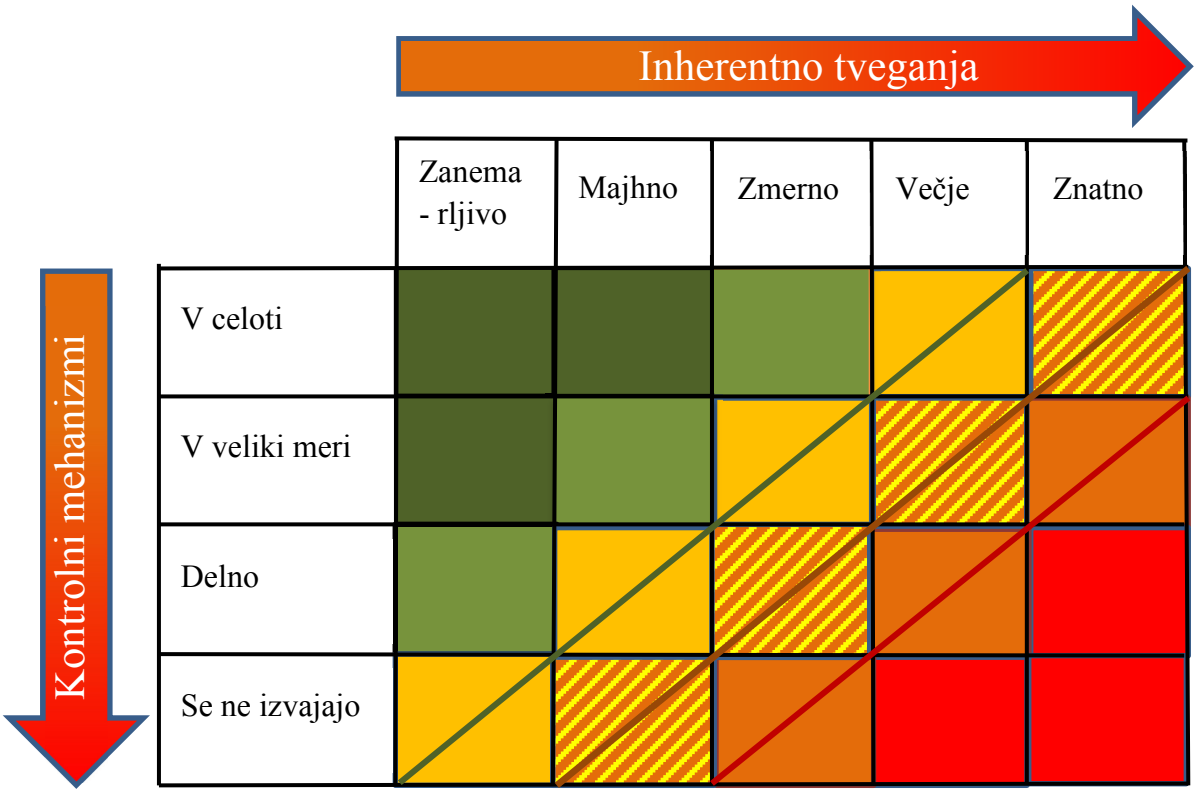
Tabela 9: Ocena kategorij in inherentnega tveganja.

Kategorija	*Št. Metrik*	Zanemarljivo 1	Majhno 2	Zmerno 3	Večje 4	Znatno 5	Povprečna ocena
Tehnologije in povezljivosti	14	21%	14%	14%	36%	14%	3,07
Dostavni kanali	3	33%	33%	0%	33%	0%	2,33
Spletni/mobilni produkti in tehn.stor.	14	21%	7%	36%	7%	29%	3,14
Organizacijske značilnosti	7	0%	29%	43%	0%	29%	3,29
Zunanje grožnje	1	0%	0%	0%	0%	100%	5,00
Povprecje:	**39**	**15%**	**17%**	**19%**	**15%**	**34%**	**3,37**

8.4 Združevanje oceni kontrolnega okolja in inherentnega tveganja

Osrednje jedro aplikacije združuje oceni kontrolnega okolja in inherentnega tveganja banke v končno oceno kibernetskega tveganja banke. Razmerje obeh ocen mora biti v obratnem sorazmerju. Torej večje kot je inherentno tveganje banke, boljši in naprednejši morajo biti kontrolni mehanizmi za identifikacijo, zaščito, zaznavanje, odzivanje in okrevanje oziroma upravljanje kibernetskega tveganja. Osrednje jedro grafično prikazuje kritična razmerja med stopnjo inherentnega tveganja in kontrolnega okolja. Najbolj kritična razmerja so obarvano rdeče, najmanj kritična pa so obarvana zeleno (Slika 9). Progasti kvadrati predstavljajo še sprejemljivo razmerje med oceno inherentnega tveganja in kontrolnega okolja. Skupna ocena kibernetskega tveganja, ki upošteva tako inherentno tveganje kot kontrolno okolje, je vsota ocene inherentnega tveganja in kontrolnega okolja. Ocena se teoretično nahaja na intervalu [2, 9] in je avtomatsko določena, ko je ocenjevanje opravljeno (vneseni vhodni podatki v sistem) in ko je izbran način združevanja. V primeru ocenjevanja večjega števila bank se lahko le-te razvrsti po tveganosti in nato ustrezno postopa v odvisnosti od nabora ukrepov, ki so na voljo.

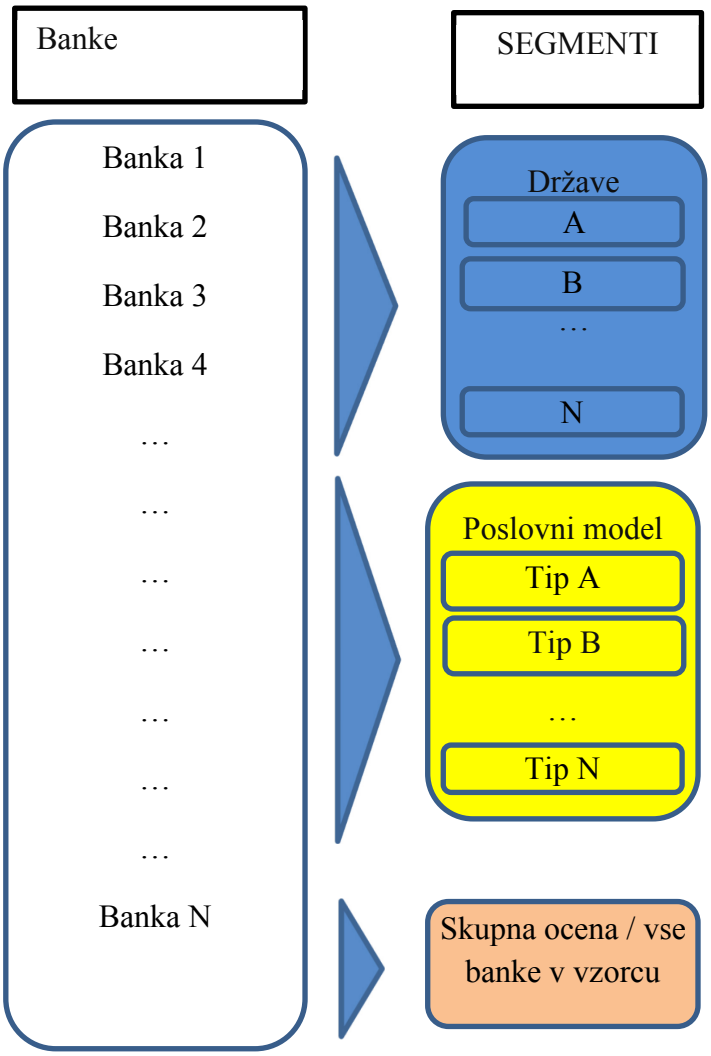
Slika 9: Združevanje oceni inherentnega tveganja in kontrolnega okolja.



8.5 Modul za nadaljnje združevanje bank po segmentih

Ko so ocenjena kibernetska tveganja za vse banke v vzorcu, je pogosto smiselno primerjati tveganja po različnih segmentih, ki so v vzorcu. Vzorec lahko nadalje razdelimo po državah ali regijah, kjer se banke nahajajo, ali po poslovnem modelu banke (npr. univerzalne banke, investicijske banke, razvojne banke, skrbniške banke itd.). Na podlagi položaja tveganja v posameznem segmentu se nato ocenjevalec/odločevalec ob pomoči sistema za podporo odločanju pri nadzoru kibernetskega tveganja v bankah odloči, na kakšen način bo postopal oziroma izbral najprimernejši način za zmanjševanje kibernetskega tveganja v določenem segmentu.

Slika 10: Združevanje bank po segmentih.



Če želimo oceniti tveganja za posamezni segment, moramo poleg načina segmentacije vse banke ustrezno razvrstiti v ustrezne segmente in nato ocene tveganj teh bank v posameznem segmentu združiti v enotno oceno. Pri tem lahko uporabimo navadno povprečje ali pa tehtano navadno povprečje glede na pomembnost banke. Kriterij pomembnosti banke je v bančnem sektorju najpogosteje velikost bilančne vsote. Kot kriterij se lahko uporabi tudi znesek danih kreditov, znesek prejetih depozitov ali število komitentov. Način združevanja je zelo podoben, če želimo združiti ocene vseh bank v enotno oceno kibernetskega tveganja za celoten vzorec. Slednje je zelo smiselno v primeru ponavljajočih meritev in zasledovanja trenda gibanja kibernetskega tveganja v celotnem vzorcu.

8.6 Razvrščanje in identifikacija

Modul »«Razvrščanje in identifikacija« razvrsti banke po tveganosti in je predzadnja enota arhitekture aplikacije sistema za podporo odločanju. Na podlagi razvrstitve se odločevalec lažje odloči v kombinaciji z ostalimi informacijami, ki jih ima na voljo, kakšni bodo naslednji koraki pri zmanjševanju, nadzorovanju oziroma upravljanju kibernetskega tveganja.

Tabela 10: Razvrstitev bank po tveganosti.

Banka	Skupaj tveganje	Inherentno tveganje	kontrolno okolje
Banka 1	7,85	3,85	4,00
Banka 2	7,60	4,60	3,00
Banka 3	7,40	4,20	3,20
Banka 4	7,30	4,10	3,20
Banka 5	7,30	4,00	3,30
Banka 6	7,25	4,15	3,10
Banka 7	7,20	3,80	3,40
Banka 8	7,00	3,70	3,30
Banka 9	7,00	3,50	3,50
Banka 10	6,80	3,90	2,90
Banka 11	6,80	3,90	2,90
Banka 12	6,70	3,90	2,80

8.7 Poročilo o tveganju in predlog ukrepov

V primeru večjega vzorca ocenjevanih bank ali pogoste izvedbe ocenjevanja je možnosti vsebinske presoje manj, s čimer večjo dobi sistem za podporo odločanju. Modul »Poročilo o tveganju in predlog ukrepov«, ki je izhodni modul sistema za podporo odločanju, izdela avtomatsko poročilo o tveganju za banke s predlogi ukrepov za banke s povečanim tveganjem. Poročilo z ukrepi se izvede le za banke, katerih skupna ocena kibernetskega tveganja presega »visoko vrednost« ali »kritično vrednost«. Obe vrednosti sta seveda odvisni od naklonjenosti tveganju oziroma od stopnje konservativnosti pri merjenju. V demonstrativnem primeru je določena vrednost 7 za kritično vrednost ocene skupnega tveganja (4 za inherentno tveganje in 3 za kontrolno okolje) ter vrednost 5,5 za visoko vrednost ocene skupnega tveganja (3 za inherentno tveganje in 2,5 za kontrolno okolja). Predlog ukrepa se vedno nanaša na aktivnosti za izboljšavo ocene osnovnega elementa bodisi pri inherentnem tveganju bodisi pri kontrolnem okolju. Postopek identifikacije elementov s kritično oziroma visoko oceno poteka v nasprotno smer kot v modulih za združevanje pri ocenjevanju inherentnega tveganja oziroma kontrolnega okolja. Torej se iz kritične oziroma visoke ocene skupnega tveganja identificirajo kritično oziroma visoko ocenjene funkcije, kategorije ter elementi inherentnega tveganja in kontrolnega okolja.

V nadaljevanju je prikazan psevdo algoritem za izdelavo poročila o tveganju za banke s predlogom ukrepov za zmanjšanje kibernetskega tveganja za tiste banke, za katere skupna ocena kibernetskega tveganja presega kritično vrednost.

Algoritem 1: Priprava poročila o tveganju in predlog ukrepov za banke, katere skupna ocena kibernetskega tveganja presega »kritično vrednost«.

```
MEJA_TVEG=7                                                    //Določitev kritične vrednosti za skupno tveganje
MEJA_INH_TVEG=4                                                //Določitev kritične vrednost i za inherentno tveganje
MEJA_KONT_TVEG=3                                               //Določitev kritične vrednosti za kontrolno okolje

For i=1 to Stevilo_bank_v_vzorcu
  If banka(i).skupno_tveganje > MEJA_TVEG then                 //Tveganje banke je kritično. Generira se poročilo
  //Generira se poročilo za banko in identificira kritične funkcije, kategorije in elemente ter predlaga ukrepe
  Generiraj_porocilo_za_banko(i)
  Dodaj_v_porocilo_za_banko(i, »Ocena kibernetskega tveganja je kritična. Razlogi so:«)
  // PREGLEDOVANJE KONTROLNEGA OKOLJA
    If banke(i).kontrolno_okolje_ocena> MEJA_KONT_TVEG then          //Kontrolno okolje je kritično

      Dodaj_v_porocilo_za_banko(i, »Kontrolno okolje je kritično. Razlogi so:«)
      For j=1 to Stevilo_funkcij_kotrolnega_okolja                   //Identificirajo se kritične funkcije
        If banke(i).fun(j).ocena > MEJA_KONT_TVEG then               //Funkcija je kritična
        Dodaj_v_porocilo_za_banko(i,»Funkcija«& banke(i).fun(j).ime & » je kritična. Razlogi so:«)
          For k=1 to banke(i).fun(j).stevilo_kategorij.              //Identificirajo se kritične kategorije
            If banke(i).fun(j).kateg(k).ocena > MEJA_KONT_TVEG then  //kategorija je kritična
              Dodaj_v_porocilo_za_banko(i,»Kategorija «& banke(i).fun(j).kateg(k).ime & »je kritična. Razlogi so:«
              For e=1 to banke(i).fun(j).kateg(k).stevilo_elementov  //Identificirajo se kritični el.
                If banke(i).fun(j).kateg(k).elem(e).ocena> MEJA_KONT_TVEG then //element je kritičen
```

```
                        Dodaj_v_porocilo_za_banko(i,»Element« & banke(i).fun(j).kateg(k). elem(e).ime & »je
                        kritičen. Predlog ukrepa:«)
                        //Za kritičen element se predlaga ukrep za zmanjšanje tveganja
                        Dodaj_ukrep_v_porocilo_za_banke(banke(i).fun(j).kateg(k).elem(e))
                    Endif
                EndFor                                              //konec Identifikacije kritičnih elementov
                Endif
            EndFor                                                  //konec Identifikacije kritičnih kategorij
        Endif
    EndFor                                                          //konec Identifikacije kritičnih funkcij
EndIf                                                               //konec pregledovanja kontrol. okolja

// PREGLEDOVANJE INHERENTNEGA TVEGANJA

If banke(i).inherento_tveganje_ocena> MEJA_INH_TVEG then            //Inherentno tveganje je kritično
    Dodaj_v_porocilo_za_banko(i, »Inherentno tveganje je kritično. Razlogi so:«)
        For k=1 to banke(i).stevilo_kategorij_inht.                 //Identificirajo se kritične kategorije
            If banke(i).kateg_inht(k).ocena > MEJA_INH_TVEG then EndIf //kategorija je kritična
            Dodaj_v_porocilo_za_banko(i,»Kategorija «& banke(i).kateg_inht(k).ime & »je kritična. Razlogi so:«
                For e=1 to banke(i).kateg_inht(k).stevilo_elementov //Identificirajo se kritični el.
                    If banke(i).kateg_inht(k).elem(e).ocena> MEJA_INH_TVEG then //element je kritičen
                        Dodaj_v_porocilo_za_banko(i,»Element« & banke(i).kateg_inht(k). elem(e).ime & »je kritičen.
                        Predlog ukrepa:«)
                        //Za kritičen element se predlaga ukrep za zmanjšanje tveganja
                        Dodaj_ukrep_v_porocilo_za_banke(banke(i).kateg_inht(k).elem(e))
                    Endif
                EndFor                                              //konec Identifikacije kritičnih elementov
            Endif
        EndFor                                                      //konec Identifikacije kritičnih kategorij
    EndIf                                                           //konec pregledovanja inherent. tveganja

EndIf                                                               //konec pregledovanja za kritične banke
EndFor                                                              //konec pregledovanja bank
```

Primer ogrodja poročila, ki ga izdela algoritem v sistemu za podporo odločanju pri nadzoru kibernetskega tveganja v bankah:

Poročilo za Banko X

Ocena kibernetskega tveganja je kritična. Razlogi so:

Kontrolno okolje je kritično. Razlogi so:

Funkcija »Identifikacija« je kritična. Razlogi so:

Kategorija »Upravljanje« je kritična. Razlogi so:

Element »Varnostna politika« je kritičen.

Predlog ukrepa: Banka mora sprejeti informacijsko varnostno politiko organizacije!

Inherentno tveganje je kritično. Razlogi so:

Kategorija »Spletni/mobilni izdelki in tehnološke storitve« je kritična.

Razlogi so:

Element »Predplačniške kartice« je kritičen.

Predlog ukrepa: Banka mora zmanjšati obseg predplačniških kartic, ki jih izdaja v imenu drugih finančnih ustanov.

---

9 Sklepne ugotovitve

Čeprav kibernetsko tveganje ni nov fenomen je zavedanje o njem v družbi še vedno nizko. Zaskrbljujoče je predvsem, da pri zaposlenih na vodstvenih položajih v podjetjih in organizacijah ni dovolj zavedanja o kibernetskemu tveganju. Za zavedanje o nevarnostih kibernetskega tveganje je nujno razumevanje kibernetskih groženj. Razumevanje pa ni mogoče brez nenehnega izobraževanja in ozaveščanja. Ozaveščanje o kibernetskih tveganjih je potrebno na vseh nivojih – tako pri končnih uporabnikih informacijskih (spletnih) storitev, ki so največkrat žrtve napada, kot tudi pri vodstvih podjetij in institucij, ki odločajo o strateških odločitvah glede kibernetske varnosti in nenazadnje pri političnih odločevalcih, ki sprejemajo generalne usmeritve in strategije na najvišji ravni. Zaradi izjemno hitrega razvoja tehnologij kibernetske grožnje ves čas spreminjajo svojo obliko in nastajajo nove. Poslovanje preko sodobnih elektronskih poti, razvoj pametnih naprav, mobilnega poslovanje in računalništva v oblakih zahtevajo nadgradnjo obstoječih protivirusnih zaščit oziroma pristopov pri obvladovanju kibernetskega tveganja. Če vodstvo institucije ne razume razsežnosti kibernetskega tveganja, je zelo velika verjetnost, da ne bo prišlo do ustreznega ozaveščanja, sprejemanja ustreznih strategij in akcijskih načrtov, investiranja v izobraževanje, v strokovnjake, v posodabljanje informacijskih sistemov, medinstitucionalnega sodelovanja in nenazadnje do namenjanja zadostne količine denarja za preprečevanje kibernetskih nevarnosti.

Ne glede na to, da je v povezavi s kibernetskim tveganjem veliko prostora za izboljšave, je dejstvo, da so bili v preteklih letih narejeni bistveni premiki na bolje tako na nacionalni kot na evropski ravni. Sem sodijo: sprejetje Evropske strategije za kibernetsko varnost [16], Evropske agende za varnost [17] in Direktive o varnosti omrežij in informacij [7] na ravni EU in sprejetje Strategije kibernetske varnosti [39], Strategije razvoja informacijske družbe do leta 2020 (Digitalna Slovenija 2020) [37], in Načrta razvoja širokopasovnih omrežij naslednje generacije do leta 2020 [38] na nacionalni ravni. Pomembno je, da se zavedanje o kibernetski varnosti povečuje in da bodo za to ustanovljene/namenjene institucije tudi v praksi izvajale poslanstvo, določeno v sprejetih strategijah in zakonodaji.

V primerjavi z ostalimi področji je v bančništvu zavedanje o kibernetskemu tveganju relativno visoko. Zaradi svoje narave so banke od nekdaj žrtve napadalcev, ki bi se radi finančno okoristili. K dodatnemu zavedanju so pripomogli tudi boleči in zelo dovršeni napadi na banke v zadnjih letih, ki so povzročili večjo finančno škodo. Tudi zaradi pomembnosti ohranjanja zaupanja varčevalcev strmijo banke h kar se da varnemu poslovanju in k ozaveščanju svojih komitentov o kibernetskih nevarnostih.

Poleg tega imajo banke zaradi stroge bančne zakonodaje in izkušenj relativno dobro izdelan sistem upravljanja tveganj. Upravljanje operativnega tveganja, v okviru katerega se obravnavajo tveganja informacijske tehnologije in kibernetska tveganja, zagotavlja osnovni okvir tudi za spremljanje kibernetskega tveganja.

Ocenjevanje, upravljanje in nadzorovanje operativnih tveganj, ki vključujejo različne vrste

tveganj od tveganj izpadov sistema, človeških napak in namernih goljufij do tako kompleksnega tveganja, kot je kibernetsko tveganje, je zapleten izziv, saj je izjemno težko definirati ustrezne metrike za merjenje tveganj. Modeliranje operativnega tveganja mora biti vedno v kombinaciji z vsebinsko presojo oziroma analizo, saj bi zanašanje zgolj na modele lahko vodilo do spregleda pomembnega vidika tveganj.

Predstavljen sistem za podporo odločanju pri nadzoru kibernetskega tveganja v bankah, bankam in bančnim nadzornim institucijam omogoča nadgrajevanje postopkov obvladovanja tveganj in programa kibernetske varnosti, vendar njenih obstoječih postopkov in programov ne nadomešča. Institucije, ki še nimajo programa kibernetske varnosti, lahko sistem uporabijo kot referenco, na podlagi katere razvijejo svoj sistem merjenja in nadzora nad kibernetskim tveganjem.

Na podlagi standardov, smernic in praks predlagana konceptualna zasnova in vsebina sistema za podporo odločanju pri nadzoru kibernetskega tveganja v bankah omogoča bankam in njenim nadzornikom skupno taksonomijo in mehanizem za opis trenutnega položaja kibernetske varnosti, opis ciljnega stanja kibernetske varnosti, identifikacijo in prioritizacijo aktivnosti za izboljšanje kibernetskega tveganja, stalni proces ocenjevanja napredka ter obveščanje med notranjimi in zunanjimi deležniki o tveganjih, povezanih s kibernetsko varnostjo.

Na koncu je potrebno poudariti, da je kibernetsko tveganje zelo dinamično, saj se kibernetske grožnje neprestano spreminjajo in izpopolnjujejo, kot se tudi spreminjajo navade, etika in ozaveščenost uporabnikov informacijskih tehnologij, zaradi česar je nujno neprestano ozaveščanje o nevarnostih kibernetskih groženj ter preverjanje in obnavljanje metodologije v skladu z najnovejšimi industrijskimi standardi.

10 Priloge

10.1 Priloga 1: Pregled obstoječih pravnih in drugih podlag

Nacionalne pravne in druge podlage, ki se nanašajo na kibernetsko varnost

- Načrt razvoja širokopasovnih omrežij naslednje generacije do leta 2020 (Sklep Vlade RS 38100-2/2016/4 z dne 10. 3. 2016) ;
- Digitalna Slovenija 2020 – Strategija razvoja informacijske družbe do leta 2020 (Sklep Vlade RS 38000-2/2015/6 z dne 10. 3. 2016);
- Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1, Ur. l. RS, št. 27/10);
- Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2012–2016; (ReNPPZK12-16, Ur. l. RS, št. 83/12);
- Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Ur. l. RS, št. 98/04-UPB1);
- Zakon o elektronskem poslovanju na trgu (ZEPT-UPB2, Ur. l. RS št. 96/2009);
- Kazenski zakonik RS (KZ-1-UPB2, Ur. l. RS št. 50/2012);
- Priporočila informacijske varnostne politike javne uprave (MJU RS, št: 386-2/2008/23, 28. 10. 2010);
- Zakon o elektronskih komunikacijah (ZEKom-1, Ur. l. RS, št. 109/12);
- Zakon o tajnih podatkih (ZTP, Ur. L. RS, št. 50/06, 9/10 in 60/11);
- Zakon o varstvu osebnih podatkov (ZVOP-1, Ur. l. RS, št. 94/07–UPB1);
- Strategija kibernetske varnosti (Sklep Vlade RS 38100-12/2015/5 z dne 25. 2. 2016);

Mednarodne pravne in druge podlage, ki se nanašajo na kibernetsko varnost

- Direktiva o varnosti omrežij in informacij(2016/1148/EU) z dne 6.7.2016;
- Direktiva o varovanju ključne infrastrukture (2008/114/EC) z dne 8.12.2008;
- Evropska agenda za varnost za obdobje 2015–2020 (COM(2015) 185) z dne 28.4.2015;
- Evropska digitalna agenda (COM(2010)245 z dne 19. 5. 2010);
- Konvencija o kibernetski kriminaliteti (ETS No.185) z dne 23.11.2001;
- Sklep Sveta EU o varnostnih predpisih za varovanju tajnih podatkov EU (Sklep št. 2013/488 /EU z dne 23. 9. 2013);
- Strategija kibernetske varnosti Evropske unije »Odprt, varen in zavarovan kibernetski prostor« z dne 7.2.2013;
- Varnostna pravila Evropske službe za zunanje delovanje (2013/C 190/01) z dne 19. 4. 2013;
- Varnostni predpisi Evropske komisije (2001/488/EC) z dne 29. 11. 2001;
- Varnostna pravila zveze NATO (C-M(2002)0049);

- Varnostna pravila zveze NATO o kibernetski varnosti (C-M(2007)0120);
- Deklaracija vrha NATA v Lizboni z dne 20. 11. 2010;
- Deklaracija vrha NATA v Chicagu z dne 20. 5. 2012.

10.2 Priloga 2: Standardi in okviri za merjenje kibernetskega tveganja

Spodaj so našteti standardi in okviri, ki se najpogosteje uporabljajo za merjenje kibernetskega tveganja, razvrščeni po pogostosti. Seznam je na podlagi raziskave pripravila delovna skupina za upravljanje s tveganji, v okviru platforme NISP [12].

- ISO 27001, ISO 27002, and ISO 27005
- ISO 31000, ISO Guide 73
- Spanish Magerit (legal requirement in Spain)
- COBIT 5
- Internally developed / adapted
- CMMI
- IT baseline security standard ISKE
- German BSI IT Baseline Protection Manual
- German BSI-Standards (100-3, 100-4)
- MONARC
- ITIL
- ISO 9001
- eBIOS

10.3 Priloga 3: Metode in orodja za merjenje kibernetskega tveganja

Spodaj je seznam metod in orodij za merjenje kibernetskega tveganja, ki jih je ENISA proučila in njihove reference objavila na spletni strani [13, 14].

Metode

- Austrian IT Security Handbook
- Cramm
- Dutch A&K Analysis
- Ebios
- ISAMM
- ISF Methods
- ISO/IEC 13335-2
- ISO/IEC 17799
- ISO/IEC 27001
- IT-Grundschutz

- Magerit
- Marion
- Mehari
- MIGRA
- Octave
- RiskSafe Assessment
- SP800-30

Orodja

- Callio
- Casis
- CCS Risk Manager
- CloudeAssurance
- Cobra
- Countermeasures
- Cramm
- EAR / PILAR
- Ebios
- GSTool
- KRiO
- ISAMM
- Mehari 2010 basic tool
- MIGRA Tool
- Modulo Risk Manager
- Octave
- Proteus
- Ra2
- REAL ISMS
- Resolver Ballot
- Resolver Risk
- Risicare
- Riskwatch
- RM Studio
- SISMS
- TRICK light
- TRICK Service
- Acuity Stream
- Axur ISMS
- WCK

10.4 Priloga 4: Seznam najpomembnejših metrik za merjenje kibernetskega tveganja

V tabelah 11, 12 in 13 so seznami najpomembnejših metrik glede na njihovo pomembnost, ki jih je pripravila delovna skupina za upravljanje s tveganji, v okviru platforme NISP [12].

Tabela 11: Metrike za merjenje kibernetskega tveganja: Prioriteta 1

Št.	Kontrola	Opis metrike
1	Varnostna ozaveščenost uporabnikov	Poraba sredstev za varnostno ozaveščenost in usposabljanje
2	Fluktuacija zaposlenih	Odstotek zaposlenih, ki zapuščajo organizacijo (na mesečni ali letni ravni)
3	Informacijsko-varnostna ozaveščenost	Odstotek osebja za informacijsko varnost, ki je bilo deležno varnostnega usposabljanja osebja s potrdilom o strokovni usposobljenosti na področju varnosti
4	Varnost tretjih oseb	Odstotek pogodb o prevzemu sistemov in storitev, ki vključujejo varnostne zahteve in/ali specifikacije in kazalnike ravni storitev
5	Varnost osebja	Odstotek posameznikov, preverjenih pred odobritvijo dostopa do občutljivih in zaupnih informacij ter sistemov
6	Varnostni proračun	Odstotek proračuna agencije za informacijski sistem, namenjenega informacijski varnosti
7	Varnost novih sistemov	Odstotek novih sistemov, ki so bili testirani in potrjeni kot skladni z najboljšimi praksami varnosti še pred njihovo izvedbo
8	Točka oddaljenega dostopa	Odstotek ogroženih točk oddaljenega dostopa
9	Uporabniški dostop	Odstotek zaposlenih, ki dobijo pooblaščen dostop do informacijskih sistemov šele, ko s podpisom potrdijo, da so prebrali in razumeli pravila obnašanja
10	Nepooblaščena naprava	Število nepooblaščenih naprav, ki so bile zaznane na omrežju ali okolju končnega uporabnika
11	Zlonamerna koda	Gibanje razmerja med številom varnostnih incidentov, ki jih je povzročila zlonamerna programska oprema in številom zaznanih in blokiranih napadov, ki jih je povzročila zlonamerna programska oprema
12	Zaščita proti zlonamerni programski opremi	Odstotek sistemov, ki so zaščiteni proti zlonamerni programski opremi

13	Fizični dostop	Odstotek mest, ki omogočajo dostop do občutljivih in zaupnih sistemov (podatkovna središča ipd.) s kontrolami fizičnega dostopa, ki ustrezajo najboljšim varnostnim standardom
14	Okoljska varnost	Odstotek naprav za okoljsko varnost (naprave za zaščito pred požari, poplavami, potresi, eksplozijami ipd.), ki se redno testirajo
15	Mobilna naprava	Odstotek mobilnih naprav, ki ustrezajo zahtevam za kibernetsko varnost organizacije
16	Upravljanje programskih popravkov	Odstotek sistemov z ažuriranim upravljanjem popravkov ali blaženjem posledic
17		Povprečni čas med razpoložljivostjo in datumom namestitve popravka
18	Sprememba	Odstotek sprememb, ki so bile pred izvedbo pregledane z vidika učinkov na varnost
19		Odstotek sprememb, ki so dobile varnostno izjemo
20	Upravljanje konfiguracij	Odstotek sistemov v sklopu upravljanja konfiguracij
21	Ranljivost	Število ranljivosti visoke stopnje, ki se po odkritju omejujejo ali upravljajo v okviru časovnih rokov, ki jih je določila organizacija
22		Povprečni čas med odkritjem ranljivosti in blaženjem njihovih posledic
23	Incident	Odstotek varnostnih incidentov (ne glede na to, kako je do njih prišlo), za katere je bilo ocenjeno, da lahko v določenem obdobju vplivajo na poslovna sredstva
24		Odstotek incidentov, obravnavanih v okviru ciljev, ki so bili dogovorjeni za raven storitev
25	Fizična varnost	Odstotek incidentov, povezanih s fizično varnostjo, ki omogočajo nepooblaščen vstop v objekte, ki vsebujejo informacijske sisteme
26	Izredne razmere	Odstotek informacijskih sistemov, ki so opravili letno testiranje načrtov ukrepov ob nepredvidljivih dogodkih
27	Skladnost konfiguracij	Odstotek sistemov v okviru upravljanja konfiguracij, ki so skladni s standardi organizacije

Vir: ENISA NISP WG1, Risk Management Best Practice, 28.4.2014.

Tabela 12: Metrike za merjenje kibernetskega tveganja: Prioriteta 2

Št.	Kontrola	Opis metrike
1	Organizacija varnosti	Število znanih in opredeljenih ključnih varnostnih vlog v upravljavskem sistemu informacijske varnosti (ISMS)
2	Vodstvena podpora	Odstotek potrditev višjih vodstvenih delavcev za strategijo kibernetske varnosti
3	Ocena kritičnih aplikacij	Odstotek aplikacij, pri katerih je bilo z oceno tveganja ugotovljeno, da so kritične za poslovne procese organizacije
4	Upravljanje s tveganji	Odstotek novih aplikacij in sistemov, za katere pred izvedbo ni bila opravljena ocena tveganja
5	Izrabljenost aplikacij	Odstotek aplikacij s pripravljenim načrtom postopnega opuščanja, vključno z arhiviranjem, izbrisom in uničenjem podatkov (kjer je primerno)
6	Uporabniški račun	Odstotek uporabnikov z dostopom do deljenih računov
7	Uporaba več računov	Odstotek uporabnikov z nepooblaščenim dostopom do več računov
8	Geslo	Delež gesel, ki ustrezajo politiki organizacije glede kakovosti gesel; ročni pregled z uporabniki ali samodejna ocena s programom za razbijanje gesel
9	Vzdrževanje	Odstotek sistemskih komponent, ki se vzdržujejo skladno s formalnimi načrti vzdrževanja
10	Ranljivost	Število ranljivosti visoke, srednje in nizke stopnje, ki so bile odkrite med rutinskimi pregledi ranljivosti in se po odkritju blažijo v časovnih rokih, ki jih je opredelila organizacija
11	Incident	Povprečni čas med nastankom in odkritjem incidenta
12		Povprečni čas med varnostnimi incidenti
13		Povprečni čas med nastankom incidenta in okrevanjem po njem
14	Politika nameščanja popravkov	Odstotek sistemov z nameščenimi popravki, kot je opredeljeno v politiki upravljanja s popravki ali politiki nameščanja popravkov
15	Pregled sistema	Število in pogostost pregledov in analize sistemov za odkrivanje nepravilnih aktivnosti

Vir: ENISA NISP WG1, Risk Management Best Practice, 28.4.2014.

Tabela 13: Metrike za merjenje kibernetskega tveganja: Prioriteta 3

Št.	Kontrola	Opis metrike
1	Kontrole stroškov incidentov	Skupni stroški incidentov v določenem časovnem obdobju
2		Povprečni stroški posameznih incidentov v določenem časovnem obdobju
3		Povprečni stroški posameznih incidentov za okrevanje po incidentu (za vzpostavitev stanja, kakršno je bilo pred incidentom)
4	Kontrole stroškov ranljivosti	Povprečni stroški posamezne ranljivosti za blaženje posledic (stroški osebja + drugi stroški)
5		Povprečni stroški za namestitev popravka (ne glede na število sistemov, ki jih to zadeva)
6	Kontrola aplikacij	Število aplikacij v organizaciji
7	Kontrola spremljanja	Odstotek (%) varnostnih sistemov, ki poročajo v sistem za upravljanje varnostnih informacij in dogodkov (ang. *Security Information and Event Monitoring – SIEM*)
8	Pregled varnosti	Število in pogostost neodvisnih pregledov informacijske varnosti

Vir: ENISA NISP WG1, Risk Management Best Practice, 28.4.2014.

10.5 Priloga 5: Seznam kategorij in elementov inherentnega tveganja

V tabeli 14 so navedeni elementi in metrike, ki jih je pri svojem orodju za ocenjevanje kibernetskega tveganja (ang. *Cybersecurity Assessment Tool*) uporabil Zvezni svet za nadzor finančnih institucij (ang. *Federal Financial Istitutions Examination Council, FFIEC*) iz ZDA [21].

Tabela 14: Seznam kategorij in elementov inherentnega tveganja.

Kategorija: Tehnologije in povezljivosti	**Zanemarljivo**	**Majhno**	**Zmerno**	**Večje**	**Znatno**
Skupno število povezav ponudnikov internetnih storitev (ISP) (vključno s podružničnimi povezavami)	Brez povezav	Majhna kompleksnost (1–20) povezav	Zmerna kompleksnost (21–100) povezav	Večja kompleksnost (101–200) povezav	Znatna kompleksnost >200 povezav
Nezavarovane zunanje povezave, (število povezav ne uporabnikov, npr. protokol za prenos datotek (FTP),Telnet, rlogin)	Brez	Malo primerov nezavarovanih povezav (1-5)	Nekaj primerov nezavarovanih povezav (6–10)	Precej primerov nezavarovanih povezav (11–25)	Znatno število primerov nezavarovanih povezav (>25)
Dostop do brezžičnega omrežja	Brez dostopa do brezžičnega omrežja	Ločene dostopne točke za gostujoča brezžična in podjetniška brezžična omrežja	Dostop do gostujočega brezžičnega omrežja je logično ločen od dostopa do podjetniškega; omejeno število uporabnikov in dostopnih točk (1–250 uporabnikov; 1–25 dostopnih točk)	Dostop do podjetniškega brezžičnega omrežja; večje število uporabnikov in dostopnih točk (251–1.000 uporabnikov; 26–100 dostopnih točk)	Dostop do podjetniškega brezžičnega omrežja; dostop imajo vsi uslužbenci; znatno število dostopnih točk (>1,000 uporabnikov; >100 dostopnih točk)
Za povezavo s podjetniškim omrežjem so dovoljene osebne naprave	Nobena	Na voljo je samo ena vrsta naprav; dostopna manj kot 5 % uslužbencem (osebju, izvršnim direktorjem, vodstvu);	Uporablja se več vrst naprav; dostopne so manj kot 10 % uslužbencem (osebju, izvršnim direktorjem,	Uporablja se več vrst naprav; dostopne so manj kot 25 % pooblaščenim uslužbencem (osebju, izvršnim	Uporablja se katerakoli vrsta naprav; dostopne so manj kot 25 % uslužbencem (osebju, izvršnim direktorjem,

Kategorija: Tehnologije in povezljivosti	Zanemarljivo	Majhno	Zmerno	Večje	Znatno
		dovoljen samo dostop do elektronske pošte	vodstvu) in upravi; dovoljen samo dostop do elektronske pošte	direktorjem, vodstvu) in upravi; dostop do elektronske pošte in nekaterih aplikacij	vodstvu) in upravi; dostop do vseh aplikacij
Tretje osebe, vključno s številom organizacij in posameznikov med prodajalci in izvajalci z dostopom do internih sistemov (npr. virtualno zasebno omrežje, modem, intranet, neposredna povezava)	Nobena tretja oseba ali posameznik iz tretjih oseb nima dostopa do sistemov	Dostop ima omejeno število tretjih oseb (1–5) in omejeno število posameznikov iz tretjih oseb (>50); nizka kompleksnost pri dostopu do sistemov	Dostop ima zmerno število tretjih oseb (6–10) in zmerno število posameznikov iz tretjih oseb (50–500); nekaj kompleksnosti pri dostopu do sistemov	Dostop ima večje število tretjih oseb (11–25) in večje število posameznikov iz tretjih oseb (501–1.500); visoka stopnja kompleksnosti pri dostopu do sistemov	Dostop ima znatno število tretjih oseb (>25) in znatno število posameznikov iz tretjih oseb (>1.500); visoka kompleksnost pri dostopu do sistemov
Veliki komitenti z namenskimi povezavami	Brez	Malo namenskih povezav (med 1–5)	Nekaj namenskih povezav (6–10)	Večje število namenskih povezav (11–25)	Znatno število namenskih povezav (>25)
Interno gostujoče in razvite ali spremenjene aplikacije prodajalcev, ki podpirajo ključne aktivnosti	Brez aplikacij	Malo aplikacij (1–5)	Nekaj aplikacij (6–10)	Večje število aplikacij (11–25)	Znatno število aplikacij in kompleksnost (>25)
Interno gostujoče aplikacije, ki so jih razvili prodajalci za podporo ključnim aktivnostim	Omejeno število aplikacij (0–5)	Malo aplikacij (6–30)	Nekaj aplikacij (31–75)	Večje število aplikacij (76–200)	Znatno število aplikacij in kompleksnost (>200)
Tehnologije, ki so jih razvili uporabniki in uporabniško programiranje, ki podpirajo ključne aktivnosti (vključno s preglednicami Microsoft Excel in podatkovnimi zbirkami Access	Brez uporabniško razvitih tehnologij	1–100 tehnologij	101–500 tehnologij	501–2.500 tehnologij	>2.500 tehnologij

Kategorija: Tehnologije in povezljivosti	Zanemarljivo	Majhno	Zmerno	Večje	Znatno
in drugimi orodji, ki so jih razvili uporabniki)					
Izrabljeni (EOL) sistemi	Brez sistemov (strojne ali programske opreme) s pretečeno življenjsko dobo oziroma tistih, ki jim bo v roku dveh let potekla življenjska doba	Malo sistemov, ki se jim izteka življenjska doba in nobenih, ki podpirajo ključno delovanje	Nekaj sistemov, ki se jim bo življenjska doba iztekla v roku dveh let in nekaj sistemov, ki podpirajo ključne operacije	Veliko število izrabljenih sistemov, ki podpirajo ključne operacije ali ki jim bo življenjska doba potekla v roku dveh let	Večina ključnih operacij je odvisna od sistemov, ki so že izrabljeni ali jim bo življenjska doba potekla v roku dveh let oziroma neznano število izrabljenih sistemov
Odprtokodna programska oprema (OPO)	Brez OPO	Omejen obseg OPO in nobene opreme, ki podpira ključne operacije	Nekaj OPO, ki podpira ključne operacije	Veliko število OPO, ki podpira ključne operacije	Večina operacij je odvisna od OPO
Omrežne naprave (npr. strežniki, usmerjevalniki in požarni zidovi; fizični in virtualni)	Z omejenim številom ali brez omrežnih naprav (<250)	Malo naprav (250– 1.500)	Nekaj naprav (1.501–25.000)	Večje število naprav (25.001–50.000)	Znatno število naprav (>50.000)
Tretji ponudniki storitev, ki hranijo in/ali obdelujejo informacije za podporo ključnih aktivnosti (nimajo dostopa do internih sistemov, vendar se ustanova zanaša na njihove storitve)	Brez tretjih oseb, ki podpirajo ključne aktivnosti	1–25 tretjih oseb, ki podpirajo ključne aktivnosti	26–100 tretjih oseb, ki podpirajo ključne aktivnosti	101–200 tretjih oseb, ki podpirajo ključne aktivnosti; 1 ali več teh je tujih	>200 tretjih oseb, ki podpirajo ključne aktivnosti; 1 ali več teh je tujih
Storitve računalništva v oblaku, ki gostujejo pri zunanjih izvajalcih, za podporo ključnih aktivnosti	Brez ponudnikov storitev v oblaku	Malo ponudnikov storitev v oblaku; samo zasebni oblak (1–3)	Nekaj ponudnikov storitev v oblaku (4–7)	Večje število ponudnikov storitev v oblaku (8–10); lokacije ponudnikov storitev v oblaku vključujejo mednarodne; uporaba javnega oblaka	Znatno število ponudnikov storitev v oblaku (>10); lokacije ponudnikov storitev v oblaku vključujejo mednarodne; uporaba javnega oblaka

Kategorija: Dostavni kanali	Zanemarljivo	Majhno	Zmerno	Večje	Znatno
Spletna stran za komitente	Nima spletnih aplikacij oziroma ni prisotna na družbenih medijih	Služi kot informativna spletna stran oziroma stran družbenega medija (obvešča npr. o podružničnih lokacijah in lokacijah bankomatov ter ponuja tržno gradivo)	Služi kot dostavni kanal pri spletnem bančnem poslovanju s fizičnimi osebami; s strankami lahko komunicira prek družbenih medijev	Služi kot dostavni kanal pri poslovanju z velikimi komitenti lahko vključuje ustvarjanje računov na področju poslovanja s fizičnimi osebami (retail account origination)	Spletne aplikacije služijo kot kanal do velikih komitentov za upravljanje s sredstvi velike vrednosti
Mobilna prisotnost	Ni prisotna na mobilnih napravah	Zgolj tekstovna SMS opozorila ali obvestila; dostop prek brskalnika	Mobilna aplikacija za bančno poslovanje s fizičnimi osebami (npr. plačevanje računov, mobilni dostop, zgolj interni prenosi)	Mobilna aplikacija za bančno poslovanje vključuje zunanje prenose (npr. za pravne osebe, ponavljajoče zunanje transakcije)	Polna funkcionalnost, vključno z originacijo novih transakcij (npr. ACH, elektronsko)
Bankomati (poslovanje)	Ne ponuja bankomatskih storitev	Ponuja bankomatske storitve, a nima lastnih bankomatov	Bankomatske storitve upravlja tretja oseba; bankomati pri krajevnih in regionalnih podružnicah; storitve polnjenja bankomatov z gotovino izvajajo zunanji izvajalci	Bankomatske storitve se upravljajo interno; bankomati v podružnicah in maloprodajnih lokacijah v državi; storitve polnjenja bankomatov z gotovino izvajajo zunanji izvajalci	Bankomatske storitve se upravljajo interno; bankomatske storitve za druge finančne ustanove; bankomati v domačih in mednarodnih podružnicah in maloprodajnih lokacijah; storitve polnjenja bankomatov z gotovino se upravljajo interno

Kategorija: Spletni/mobilni izdelki in tehnološke storitve	Zanemarljivo	Majhno	Zmerno	Večje	Znatno
Debetne in kreditne kartice	Ne izdaja debetnih ali kreditnih kartic	Debetne ali kreditne kartice izdaja prek tretjih oseb; <10,000 kartic	Debetne ali kreditne kartice izdaja prek tretjih oseb; 10.000–50.000 kartic	Debetne ali kreditne kartice izdaja direktno 50.001–100.000	Debetne ali kreditne kartice izdaja direktno >100.000; kartice izdaja v imenu drugih finančnih ustanov;
Predplačniške kartice	Ne izdaja predplačniških kartic	Predplačniške kartice izdaja prek tretjih oseb; <5,000 kartic	Predplačniške kartice izdaja prek tretjih oseb; 5.000–10.000 kartic	Predplačniške kartice izdaja prek tretjih oseb; 10.001–20.000	predplačniške kartice izdaja interno, prek tretje osebe ali v imenu drugih finančnih ustanov; >20.000
Nastajajoče plačilne tehnologije (npr. digitalne denarnice, mobilne denarnice)	Ne sprejema ali uporablja nastajajočih plačilnih tehnologij	Posredno sprejema ali uporablja nastajajoče plačilne tehnologije (uporaba teh tehnologij pri strankah lahko vpliva na depozitni ali kreditni račun)	Neposredno sprejema ali uporablja nastajajoče plačilne tehnologije; partnerstvo ali sodelovanje z nebančnimi izvajalci; omejen obseg transakcij	Neposredno sprejema ali uporablja nastajajoče plačilne tehnologije; majhen obseg transakcij; brez mednarodnega plačilnega prometa	Neposredno sprejema nastajajoče plačilne tehnologije; zmeren obseg transakcij in/ali mednarodnega plačilnega prometa
Plačila med dvema fizičnima osebama (P2P)	Ne ponuja	Strankam je dovoljeno ustvariti plačila; to možnost uporablja <1.000 strank oziroma obseg mesečnih transakcij je <50.000	Strankam je dovoljeno iniciirati plačila; to možnost uporablja 1.000–5.000 strank oziroma obseg mesečnih transakcij je 50.000-100.000	Strankam je dovoljeno iniciirati plačila; to možnost uporablja 5.001–10.000 strank oziroma obseg mesečnih transakcij je 100.001–1 milijon	Strankam je dovoljeno zahtevati ali iniciirati plačilo; to možnost uporablja >10.000 strank oziroma obseg mesečnih transakcij je >1 milijon
Iniciiranje plačil ACH	ACH ne nastopa kot iniciator	izdaja naloge za dobropise ; dnevni obseg <3 % bilančne vsote	Izdaja naloge za obremenitve in dobropise; dnevni obseg je 3–5 % bilančne vsote	Podpira procesiranje plačil za tretje osebe; izdaja naloge za obremenitve in dobropise, z dnevnim obsegom v višini 6-25% bilančne vsote	Podpira procesiranje plačil za tretje osebe; izdaja naloge za obremenitve in dobropise z dnevnim obsegom, ki presega 25% bilančne vsote

Kategorija: Spletni/mobilni izdelki in tehnološke storitve	Zanemarljivo	Majhno	Zmerno	Večje	Znatno
Izdaja nalogov za plačila med velikimi komitenti (npr. CHIPS)	Ne izdaja nalogov za plačila med velikimi komitenti	Dnevni obseg nalogov za plačila med velikimi komitenti <3 % skupnih sredstev	Dnevni obseg nalogov za plačila med velikimi komitenti znaša 3–5 % skupnih sredstev	Dnevni obseg nalogov za plačila med velikimi komitenti znaša 6–25 % skupnih sredstev	Dnevni obseg nalogov za plačila med velikimi komitenti presega 25 % skupnih sredstev
Elektronski prenosi sredstev	Ne ponuja	Samo osebne zahteve za elektronski prenos; samo domači elektronski prenosi; dnevni obseg elektronskih prenosov <3 % skupnih sredstev	Zahteve so podane osebno, prek telefona ali faksa; dnevni obseg domačih elektronskih prenosov znaša 3-5 % skupnih sredstev; dnevni obseg mednarodnih elektronskih prenosov <3 % skupnih sredstev	Različni kanali za zahteve (npr. prek spleta, tekstovni, el. pošta, faks in telefon); dnevni obseg domačih elektronskih prenosov znaša 6–25 % skupnih sredstev; dnevni obseg mednarodnih elektronskih prenosov znaša 3–10 % skupnih sredstev	Različni kanali za zahteve (npr. prek spleta, tekstovni, elektronska pošta, faks in telefon); dnevni obseg domačih elektronskih prenosov >25 % skupnih sredstev dnevni obseg mednarodnih elektronskih prenosov >10 % skupnih sredstev
Zajem depozitov preko oddaljenega dostopa za trgovce (ang: Merchant remote deposit capture – RDC)	Ne ponuja RDC za trgovce	<100 strank trgovcev; dnevni obseg transakcij znaša <3 % skupnih sredstev	100–500 strank trgovcev; dnevni obseg transakcij znaša 3–5 % skupnih sredstev	501–1.000 strank trgovcev; dnevni obseg transakcij znaša 6–25 % skupnih sredstev	>1.000 strank trgovcev; dnevni obseg transakcij znaša >25 % skupnih sredstev
Svetovna nakazila	Ne ponuja svetovnih nakazil	Bruto dnevni obseg transakcij znaša <3 % skupnih sredstev	Bruto dnevni obseg transakcij znaša 3–5 % skupnih sredstev	Bruto dnevni obseg transakcij znaša 6–25 % skupnih sredstev	Bruto dnevni obseg transakcij znaša >25 % skupnih sredstev
Storitve zakladništva za stranke	Ne ponuja upravljanja storitev zakladništva	Ponuja omejene storitve; število strank <1.000	Ponujene storitve vključujejo uporabo poštnih predalov (lockbox), izdajanje nalogov prek ACH ter zajem depozitov na daljavo; število strank je 1.000–10.000	Ponujene storitve vključujejo rešitve za terjatve in upravljanje likvidnosti; število strank je 10.001–20.000	Ponuja več storitev, vključno z valutnimi storitvami, spletnimi naložbami in avtomatski prenos sredstev med naložbenimi računi (ang: investment sweep accounts); število strank je >20.000

Kategorija: Spletni/mobilni izdelki in tehnološke storitve	Zanemarljivo	Majhno	Zmerno	Večje	Znatno
Skrbniške storitve	Ne ponuja skrbniških storitev	Skrbniške storitve ponuja prek tretjega ponudnika storitev; upravljana sredstva znašajo <500 milijonov dolarjev	Skrbniške storitve zagotavlja neposredno; portfelj upravljanih sredstev znaša 500–999 milijonov dolarjev	Skrbniške storitve zagotavlja neposredno; upravljana sredstva znašajo 1–10 milijard dolarjev	Skrbniške storitve zagotavlja neposredno; upravljana sredstva znašajo >10 milijard dolarjev
Deluje kot korespondenčna banka (medbančni prenosi)	Ne deluje kot korespondenčna banka	Deluje kot korespondenčna banka za <100 ustanov	Deluje kot korespondenčna banka za 100–250 ustanov	Deluje kot korespondenčna banka za 251–500 ustanov	Deluje kot korespondenčna banka za >500 ustanov
Pridobivanje trgovcev (podpiranje trgovcev ali dejavnost obdelovanja kartic v plačilni sistem)	Ne pridobiva trgovcev	Pridobiva trgovce; <1.000 trgovcev	Pridobiva trgovce; obdelavo plačil s karticami opravlja zunanji izvajalec; 1.000-10.000 trgovcev	Pridobiva trgovce in obdeluje plačila s karticami; 10.001–100.000 trgovcev	Pridobiva trgovce in obdeluje plačila s karticami; >100.000 trgovcev
Omogoča gostovanje IT storitev za druge organizacije (bodisi prek skupnih sistemov ali z administrativno podporo)	Ne zagotavlja IT storitev za druge organizacije	Omogoča gostovanje ali zagotavlja IT storitve za povezane organizacije	Omogoča gostovanje ali zagotavlja IT storitve za do 25 nepovezanih organizacij	Omogoča gostovanje ali zagotavlja IT storitve za 26–50 nepovezanih organizacij	Omogoča gostovanje ali zagotavlja IT storitve za >50 nepovezanih organizacij

Kategorija: Organizacijske značilnosti	Zanemarljivo	Majhno	Zmerno	Večje	Znatno
Združitve in prevzemi (vključno z odprodajami in skupnimi podjemi)	Ne načrtuje	Sprejema možnost za začetek pogovorov oziroma dejavno išče priložnosti za združitev ali prevzem	Sodeluje v pogovorih z vsaj 1 stranko	Javna objava prodaje ali prevzema v zadnjem letu, pogajanja z eno ali več strankami	V teku je več postopkov integracije prevzemov
Zaposleni (vključno z izvajalci storitev informacijske tehnologije in kibernetske varnosti)	<50 zaposlenih	Število zaposlenih znaša 50–2000	2.001–10.000 zaposlenih	10.001–50.000 zaposlenih	>50.000 zaposlenih

Kategorija: Organizacijske značilnosti	Zanemarljivo	Majhno	Zmerno	Večje	Znatno
Spremembe v osebju, ki izvaja storitve IT in informacijske varnosti	Ključna mesta so zasedena; malo ali nič menjav osebja	Prosta so delovna mesta za neključno osebje	Nekaj menjav na ključnih ali vodilnih delovnih mestih	Pogoste menjave na ključnih ali vodilnih delovnih mestih	Vodilna ali ključna delovna mesta ostajajo nezasedena za dolgo obdobje; pogoste menjave osebja na področju IT in informacijske varnosti
Privilegiran dostop (administratorji – omrežje, podatkovna zbirka, aplikacije, sistemi itd.)	Omejeno število administratorjev; omejeno število ali nič zunanjih administratorjev	Obseg menjav administratorjev ne vpliva na poslovanje ali dejavnosti; lahko uporabijo nekaj zunanjih administratorjev	Obseg menjav administratorjev vpliva na poslovanje; število administratorjev za posamezne sisteme ali aplikacije presega potrebe	Visoka stopnja odvisnosti od zunanjih administratorjev; število administratorjev ne zadošča obsegu ali hitrosti sprememb	Visoka stopnja menjav omrežnih skrbnikov; mnogo ali večina administratorjev/ skrbnikov je zunanjih (podizvajalci ali prodajalci); omejene izkušnje z administriranjem omrežij
Spremembe v IT okolju (npr. omrežje, infrastruktura, ključne aplikacije, podporne tehnologije za nove izdelke ali storitve)	Stabilno IT okolje	Redke ali minimalne spremembe v IT okolju	Redno sprejemanje novih tehnologij	Velik obseg večjih sprememb	Znatne spremembe na področju podizvajalcev ključnih storitev IT; pogoste obsežne in kompleksne spremembe v okolju
Lokacije podružnic/poslovna prisotnost	1 mesto	1 regija	1 država	1–20 držav	>20 držav
Lokacije poslovanja/podatkovna središča	1 mesto	1 regija	1 država	1–10 držav	>10 držav

Kategorija: Zunanje grožnje	Zanemarljivo	Majhno	Zmerno	Večje	Znatno
Poskusi kibernetskih napadov	Ni poskusov napadov ali izvidništva	Malo mesečnih poskusov (<100); možnost, je bila žrtev generičnih kampanj lažnega predstavljanja (phishing) usmerjenih na uslužbence in stranke	Nekaj mesečnih poskusov (100–500); kampanje ribarjenja, usmerjene na uslužbence ali stranke ustanove ali na tretje izvajalce podpore ključnih aktivnosti; možnost, da so bili v zadnjem letu žrtve poskusa porazdeljene zavrnitve storitve (DDoS)	Večje število mesečnih poskusov (501–100.000); usmerjenega lažnega predstavljanja (spear phishing campaigns), ki se osredotoča na stranke visoke neto vrednosti v ustanovi ali tretje izvajalce podpore ključnih aktivnosti; ustanova je izrecno omenjena v poročilih o grožnjah; možnost, da so bili v zadnjem letu žrtve večkratnih poskusov DDoS napadov	Znatno število mesečnih poskusov (>100.000); vztrajni poskusi napadov na višje vodstvene položaje in/ali skrbnike omrežij; pogosta tarča napadov DDoS

Vir: Cybersecurity Assessment Tool (FFIEC).

10.6 Priloga 6: Seznam funkcij, kategorij in elementov kontrolnega okolja

Iz tabele 15 je razvidna segmentacija kontrolnih mehanizmov na funkcije, kategorije in podkategorije, ki jih je predlagal Nacionalni inštituta za standarde in tehnologijo (NIST) iz ZDA v izdanem Okviru za izboljšanje kibernetske varnosti kritične infrastrukture (ang. *Framework for Improving Critical Infrastructure Cybersecurity*) [26].

Tabela 15. Seznam funkcij, kategorij in elementov kontrolnega okolja.

Funkcija	Kategorija	Podkategorija	Informativne reference
IDENTIFIKACIJA (ID)	Upravljanje sredstev (ID.AM): Določijo se podatki, osebje, naprave, sistemi in objekti, ki organizaciji omogočajo doseganje poslovnih namenov in se upravljajo skladno z njihovim relativnim pomenom za njene poslovne cilje in strategijo obvladovanja tveganj.	ID.AM-1: Popišejo se fizične naprave in sistemi v organizaciji.	CCS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Popišejo se programske platforme in aplikacije v organizaciji.	CCS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Mapirajo se organizacijski komunikacijski in podatkovni tokovi.	CCS CSC 1 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Pripravi se katalog zunanjih informacijskih sistemov.	COBIT 5 APO02.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Določijo se prednostni viri (npr. strojna oprema, naprave, podatki in programska oprema) glede na njihovo razvrstitev, ključnost in poslovno vrednost.	COBIT 5 APO03.03, APO03.04, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Vzpostavijo se vloge in odgovornosti na področju kibernetske varnosti za vso	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1

Funkcija	Kategorija	Podkategorija	Informativne reference
		delovno silo in tretje deležnike (npr. dobavitelje, stranke, partnerje).	NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	Poslovno okolje (ID.BE): Organizacija razume in prednostno obravnava svoje poslanstvo, cilje, deležnike in dejavnosti; te informacije se uporabijo pri oblikovanju vlog in odgovornosti na področju kibernetske varnosti ter odločitev povezanih z obvladovanjem tveganj.	ID.BE-1: Prepozna in sporoča se vloga organizacije v dobavni verigi.	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: Ugotovi in sporoči se položaj organizacije v kritični infrastrukturi in v njenem sektorju.	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Določijo in sporočijo se prednostne naloge za poslanstvo, cilje in aktivnosti organizacije.	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Ugotovijo se odvisnosti in ključne funkcije za zagotavljanje ključnih storitev.	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Za podporo zagotavljanja ključnih storitev se določijo zahteve za odpornost.	COBIT 5 DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
	Upravljanje (ID.GV): Organizacija razume politike, postopke in procese za obvladovanje in spremljanje regulatornih, zakonskih, okoljskih in poslovnih zahtev ter zahtev za obvladovanje tveganj in jih upošteva pri obvladovanju varnostnih tveganj v kibernetskem prostoru.	ID.GV-1: Vzpostavljena je informacijska varnostna politika.	COBIT 5 APO01.03, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1
		ID.GV-2: Vloge in odgovornosti na področju informacijske varnosti se koordinirajo in usklajujejo z internimi vlogami in zunanjimi partnerji.	COBIT 5 APO13.12 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 NIST SP 800-53 Rev. 4 PM-1, PS-7
		ID.GV-3: Organizacija razume in obvladuje zakonske in	COBIT 5 MEA03.01, MEA03.04

Funkcija	Kategorija	Podkategorija	Informativne reference
		regulatorne zahteve na področju kibernetske varnosti, vključno z obveznostmi glede zasebnosti in državljanskih svoboščin.	ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1 NIST SP 800-53 Rev. 4 -1 kontrole iz vseh družin (razen PM-1)
		ID.GV-4: Postopki upravljanja in obvladovanja tveganj obravnavajo kibernetska varnostna tveganja.	COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 NIST SP 800-53 Rev. 4 PM-9, PM-11
	Ocena tveganja (ID.RA): Organizacija razume kibernetska varnostna tveganja, ki jim je izpostavljeno njeno delovanje (vključno s poslanstvom, funkcijami, podobo ali ugledom), njeno premoženje in posamezniki.	ID.RA-1: Prepoznajo in dokumentirajo se ranljivosti premoženja.	CCS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.23.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Informacije o grožnjah in ranljivosti prejema od forumov in virov za izmenjavo informacij.	ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5
		ID.RA-3: Prepoznavanje in dokumentiranje groženj, tako notranjih kot zunanjih.	COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Prepoznavanje verjetnosti in možnosti potencialnih vplivov na poslovanje.	COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Grožnje, ranljivosti, verjetnosti in učinki se uporabijo pri določanju tveganja.	COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		ID.RA-6: Prepoznavanje in prednostna obravnava odzivov na tveganja.	COBIT 5 APO12.05, APO13.02 NIST SP 800-53 Rev. 4 PM-4, PM-9

Funkcija	Kategorija	Podkategorija	Informativne reference
	Strategija upravljanja s tveganji (ID.RM): Organizacija določi prednostne naloge, omejitve, dovoljeno tveganje in predpostavke ter jih uporabi za podporo pri odločanju na področju operativnega tveganja.	ID.RM-1: Deležniki organizacije določijo in upravljajo postopke obvladovanja tveganj in se dogovarjajo o njih.	COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 NIST SP 800-53 Rev. 4 PM-9
		ID.RM-2: Določitev in jasna opredelitev dovoljenega tveganja organizacije.	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 NIST SP 800-53 Rev. 4 PM-9
		ID.RM-3: Dovoljeno tveganje organizacije se določi glede na njeno vlogo v kritični infrastrukturi in analizo tveganj, povezanih s sektorjem.	NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
PROTECT (PR)	Nadzor dostopa (PR.AC): Dostop do sredstev in povezanih objektov je omejen na pooblaščene uporabnike, postopke ali naprave ter na pooblaščene dejavnosti in transakcije.	PR.AC-1: Upravljanje identitet in referenc za pooblaščene naprave in uporabnike.	CCS CSC 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-2, IA
		PR.AC-2: Vzdržuje in zaščiti se fizični dostop do sredstev.	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE5, PE-6, PE-9
		PR.AC-3: Vzdržuje se dostop na daljavo.	COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
		PR.AC-4: Upravljanje dovoljenj za dostop z vključevanjem načel najmanjšega privilegija in ločevanja nalog.	CCS CSC 12, 15 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1,

Funkcija	Kategorija	Podkategorija	Informativne reference
			A.9.4.4 NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: Zaščiti se celovitost omrežja, po potrebi tudi s segregacijo omrežja.	ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, SC-7
	Ozaveščanje in usposabljanje (PR.AT): Organizacija za svoje osebje in partnerje zagotovi izobraževanje s področja ozaveščanja o kibernetski varnosti in jih ustrezno usposablja za izvajanje njihovih dolžnosti in nalog povezanih z informacijsko varnostjo, skladno z ustreznimi politikami, postopki in dogovori.	PR.AT-1: Vsi uporabniki so obveščeni in usposobljeni.	CCS CSC 9 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2 NIST SP 800-53 Rev. 4 AT-2, PM-13
		PR.AT-2: Privilegirani uporabniki razumejo vloge in odgovornosti.	CCS CSC 9 COBIT 5 APO07.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-3: Tretji deležniki (npr. dobavitelji, stranke, partnerji) razumejo vloge in odgovornosti.	CCS CSC 9 COBIT 5 APO07.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9
		PR.AT-4: Višji vodstveni delavci razumejo vloge in odgovornosti.	CCS CSC 9 COBIT 5 APO07.03
			ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-5: Varnostno osebje zadolženo za fizično in informacijsko varnost razume vloge in odgovornosti.	CCS CSC 9 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1,

Funkcija	Kategorija	Podkategorija	Informativne reference
			A.7.2.2, NIST SP 800-53 Rev. 4 AT-3, PM-13
	Varnost podatkov (PR.DS): Informacije in evidence (podatki) se upravljajo skladno s strategijo organizacije za obvladovanje tveganj da se zaščiti zaupnost, celovitost in dostopnost informacij.	PR.DS-1: Podatki v mirovanju (data-at-rest) so zaščiteni.	CCS CSC 17 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 SC-28
		PR.DS-2: Tranzitni podatki so zaščiteni.	CCS CSC 17 COBIT 5 APO01.06, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8
		PR.DS-3: Formalno upravljanje sredstev skozi postopke odstranitve, prenosov in odsvojitve.	COBIT 5 BAI09.03 ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-4: Vzdrževanje ustrezne zmogljivosti za zagotavljanje dostopnosti.	COBIT 5 APO13.01 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.12.3.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.DS-5: Izvaja se zaščita proti odtekanju podatkov.	CCS CSC 17 COBIT 5 APO01.06 ISA 62443-3-3:2013 SR 5.2 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3

Funkcija	Kategorija	Podkategorija	Informativne reference
			NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Mehanizmi za preverjanje celovitosti se uporabljajo za potrjevanje celovitosti programske opreme, sistemske programske opreme in informacij.	ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SI-7
		PR.DS-7: Razvojna in testna okolja so ločena od produkcijskega okolja.	COBIT 5 BAI07.04 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 4 CM-2
	Procesi in postopki za zaščito informacij (PR.IP): Varnostne politike (ki obravnavajo namen, obseg, vloge, odgovornosti, zavezanost vodstva in usklajevanje med subjekti organizacije), procesi in postopki se vodijo in uporabljajo pri upravljanju zaščite informacijskih sistemov in sredstev.	PR.IP-1: Oblikovanje in vzdrževanje osnovne konfiguracije sistemov informacijske tehnologije/industrijskih kontrolnih sistemov.	CCS CSC 3, 10 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Za upravljanje sistemov se izvede življenjski cikel razvoja Aplikacije.	COBIT 5 APO13.01 ISA 62443-2-1:2009 4.3.4.3.3 ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5
		PR.IP-3: Vzpostavljeni so postopki za nadzor sprememb konfiguracij.	NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA10, SA-11, SA-12, SA-15, SA-17, PL-8
			COBIT 5 BAI06.01, BAI01.06 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10

Funkcija	Kategorija	Podkategorija	Informativne reference
		PR.IP-4: Izdelajo se varnostne kopije informacij, ki se vzdržujejo in redno preverjajo.	COBIT 5 APO13.01 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
		PR.IP-5: Izpolnjene so zahteve politike in predpisov glede fizičnega operacijskega okolja za organizacijska sredstva.	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Podatki se uničijo skladno s politiko.	COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.4.4.4 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 NIST SP 800-53 Rev. 4 MP-6
		PR.IP-7: Postopki zaščite se stalno izboljšujejo.	COBIT 5 APO11.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Učinkovitost zaščitnih tehnologij se deli z ustreznimi osebami.	ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
		PR.IP-9: Vzpostavi in upravlja se z načrti odzivanja (odzivanje na incidente in neprekinjeno poslovanje) in načrti okrevanja (okrevanje po incidentih in okrevanje po nesrečah).	COBIT 5 DSS04.03 ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 NIST SP 800-53 Rev. 4 CP-2, IR-8
		PR.IP-10: Testirajo se načrti odzivanja in okrevanja.	ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 3.3

Funkcija	Kategorija	Podkategorija	Informativne reference
			ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14
		PR.IP-11: Kibernetska varnost je vključena v postopke kadrovske službe (npr. odstranjevanje identitete, preverjanje osebja).	COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 NIST SP 800-53 Rev. 4
		PR.IP-12: Razvije in izvaja se načrt obvladovanja ranljivosti.	ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
	Vzdrževanje (PR.MA): Vzdrževanje in popravila komponent sistema industrijske kontrole in informacijskega sistema se izvaja skladno s politikami in postopki.	PR.MA-1: Vzdrževanje in popravila organizacijskih sredstev se izvajajo in zabeležijo pravočasno, z odobrenimi in nadzorovanimi orodji.	COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.7 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
		PR.MA-2: Vzdrževanje organizacijskih sredstev na daljavo se odobri, zabeleži in izvaja tako, da se prepreči neavtoriziran dostop.	COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4
	Zaščitna tehnologija (PR.PT): Upravljanje z rešitvami tehnične varnosti za zagotovitev varnosti in odpornosti sistemov in sredstev, skladno z ustreznimi politikami, postopki in dogovori.	PR.PT-1: Skladno z politiko se določijo, dokumentirajo, izvajajo in pregledujejo revizijski in dnevniški zapisi.	CCS CSC 14 COBIT 5 APO11.04 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 družina AU
		PR.PT-2: Izmenljivi mediji so zaščiteni, njihova raba pa omejena skladno s politiko.	COBIT 5 DSS05.02, APO13.01 ISA 62443-3-3:2013 SR 2.3 ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9

Funkcija	Kategorija	Podkategorija	Informativne reference
			NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7
		PR.PT-3: Dostop do sistemov in sredstev je nadzorovan in vključuje načelo najmanjše funkcionalnosti.	COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 4 AC-3, CM-7
		PR.PT-4: Zaščitijo se komunikacije in nadzorna omrežja.	CCS CSC 7 COBIT 5 DSS05.02, APO13.01 ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
ZAZNAVANJE (DE)	Anomalije in dogodki (DE.AE): Pravočasno zaznavanje anomalij in razumevanje potencialnega vpliva dogodkov.	DE.AE-1: Vzpostavi in upravlja se izhodišče za omrežne operacije in pričakovane tokove podatkov za uporabnike in sisteme.	COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Zaznani dogodki se analizirajo za razumevanje tarč in metod napada.	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2

Funkcija	Kategorija	Podkategorija	Informativne reference
			ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Podatki o dogodkih se združijo in povežejo iz različnih virov in senzorjev.	ISA 62443-3-3:2013 SR 6.1 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR5, IR-8, SI-4
		DE.AE-4: Ugotovi se učinek dogodkov.	COBIT 5 APO12.06 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI 4
		DE.AE-5: Določijo se mejne vrednosti za opozarjanje o incidentih.	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.2.3.10 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
	Stalni nadzor varnosti (DE.CM): Spremljanje informacijskega sistema in sredstev v ločenih obdobjih za ugotavljanje dogodkov, povezanih s kibernetsko varnostjo in potrjevanje učinkovitosti zaščitnih ukrepov.	DE.CM-1: Spremljanje omrežja za zaznavanje potencialnih dogodkov, povezanih s kibernetsko varnostjo.	CCS CSC 14, 16 COBIT 5 DSS05.07 ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: Fizično okolje se nadzoruje z namenom zaznavanja potencialnih dogodkov, povezanih s kibernetsko varnostjo.	ISA 62443-2-1:2009 4.3.3.3.8 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE20
		DE.CM-3: Aktivnosti osebja se spremljajo z namenom zaznavanja potencialnih dogodkov, povezanih s kibernetsko varnostjo.	ISA 62443-3-3:2013 SR 6.2 ISO/IEC 27001:2013 A.12.4.1 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Zaznano je delovanje zlonamerne kode.	CCS CSC 5 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3
		DE.CM-5: Zaznana je neavtorizirana mobilna koda.	ISA 62443-3-3:2013 SR 2.4 ISO/IEC 27001:2013 A.12.5.1 NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44

Funkcija	Kategorija	Podkategorija	Informativne reference
		DE.CM-6: Izvaja se spremljanje aktivnosti zunanjega ponudnika internetnih storitev z namenom zaznavanja potencialnih dogodkov, povezanih s kibernetsko varnostjo.	COBIT 5 APO07.06 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA9, SI-4
		DE.CM-7: Izvaja se spremljanje in nadzor za zaznavanje nepooblaščenega osebja, povezav, naprav in programske opreme.	NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Izvaja se preverjanje ranljivosti.	COBIT 5 BAI03.10 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5
	Procesi zaznavanja (DE.DP): Procesi in postopki zaznavanja se izvajajo in testirajo za zagotovitev pravočasne in ustrezne seznanjenosti z anomalijami.	DE.DP-1: Za zagotovitev odgovornosti se jasno opredelijo vloge in pristojnosti za zaznavanje.	CCS CSC 5 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
		DE.DP-2: Aktivnosti zaznavanja so skladne z vsemi veljavnimi zahtevami.	ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Testirajo se postopki zaznavanja.	COBIT 5 APO13.02 ISA 62443-2-1:2009 4.4.3.2 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Informacije o zaznavanju dogodkov se posredujejo ustreznim osebam.	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.9 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Postopki zaznavanja se stalno izboljšujejo.	COBIT 5 APO11.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Funkcija	Kategorija	Podkategorija	Informativne reference
ODZIVANJE (RS)	Načrtovanje odzivov (RS.RP): Procesi in postopki odzivanja se izvajajo in vzdržujejo za zagotovitev pravočasnega odziva na zaznane varnostne dogodke v kibernetskem prostoru.	RS.RP-1: Načrt odziva se izvede med dogodkom ali po njem.	COBIT 5 BAI01.10 CCS CSC 18 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR- 8
	Komunikacije (RS.CO): Aktivnosti odzivanja se usklajujejo z notranjimi in zunanjimi deležniki kot je ustrezno za vključitev zunanje podpore organov pregona.	RS.CO-1: Osebje je seznanjeno s svojo vlogo in vrstnim redom operacij, ko nastopi potreba po odzivu.	ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Dogodki se sporočajo skladno z opredeljenimi merili.	ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
		RS.CO-3: Izmenjava podatkov se izvaja skladno z načrti odzivanja.	ISA 62443-2-1:2009 4.3.4.5.2 ISO/IEC 27001:2013 A.16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Usklajevanje z deležniki poteka skladno z načrti odzivanja.	ISA 62443-2-1:2009 4.3.4.5.5 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.CO-5: Poteka prostovoljna izmenjava informacij z zunanjimi deležniki z namenom doseganja širše ozaveščenosti o stanju kibernetske varnosti.	NIST SP 800-53 Rev. 4 PM-15, SI-5
	Analiza (RS.AN): Analiza se izvaja za zagotovitev ustreznega odziva in podporo aktivnostim okrevanja.	RS.AN-1: Raziščejo se obvestila iz sistemov odkrivanja.	COBIT 5 DSS02.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR- 5, PE-6, SI-4
		RS.AN-2: Razume se vpliv in učinek incidenta.	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISO/IEC 27001:2013 A.16.1.6

Funkcija	Kategorija	Podkategorija	Informativne reference
			NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-3: Opravi se forenzična preiskava.	ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4: Incidenti se razvrstijo skladno z načrti odzivanja.	ISA 62443-2-1:2009 4.3.4.5.6 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
	Ublažitev posledic (RS.MI): Izvajajo se aktivnosti za preprečevanje razširjanja dogodka, omejevanje njegovih učinkov in odpravo incidenta.	RS.MI-1: Zajezitev incidentov.	ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Blaženje posledic incidentov.	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3: Na novo ugotovljene ranljivosti se blažijo oziroma dokumentirajo kot sprejeta tveganja.	ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	Izboljšave (RS.IM): Aktivnosti odzivanja organizacije se izboljšujejo z vključevanjem izkušenj pridobljenih med tekočimi in preteklimi aktivnostmi odkrivanja/odzivanja.	RS.IM-1: Načrti odzivanja upoštevajo pridobljene izkušnje.	COBIT 5 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.IM-2: Strategije odzivanja se posodobijo.	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
OKREVANJE (RC)	Načrtovanje okrevanja (RC.RP): Procesi in postopki okrevanja se izvajajo in vzdržujejo za zagotovitev pravočasne obnove sistemov ali sredstev, ki so bili tarča varnostnih dogodkov v kibernetskem prostoru.	RC.RP-1: Načrt okrevanja se izvede med dogodkom ali po njem.	CCS CSC 8 COBIT 5 DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5
			NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Izboljšave (RC.IM): Načrtovanje in proces okrevanja se izboljšuje z vključevanjem pridobljenih izkušenj v prihodnje	RC.IM-1: Načrti okrevanja upoštevajo pridobljene izkušnje.	COBIT 5 BAI05.07 ISA 62443-2-1:2009 4.4.3.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

Funkcija	Kategorija	Podkategorija	Informativne reference
	aktivnosti.	RC.IM-2: Strategije okrevanja se posodobijo.	COBIT 5 BAI07.08 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	Komunikacije (RC.CO): Aktivnosti obnove se usklajujejo z notranjimi in zunanjimi deležniki, kot so centri za koordinacijo, ponudniki internetnih storitev, lastniki napadalnih sistemov, žrtvami, drugimi skupinami za odzivanje na računalniške varnostne incidente in prodajalci.	RC.CO-1: Vodijo se odnosi z javnostmi.	COBIT 5 EDM03.02
		RC.CO-2: Ugled po dogodku se popravi.	COBIT 5 MEA03.02
		RC.CO-3: Aktivnosti okrevanja se sporočajo notranjim deležnikom ter izvršilnim in vodstvenim skupinam.	NIST SP 800-53 Rev. 4 CP-2, IR-4

Vir: Framework for Improving Critical Infrastructure Cybersecurity (NIST).

11 Viri in literatura

[1] BCBS, Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches, June 2011.

[2] Bendovschi, Cyber-Attacks – Trends, Patterns and Security Countermeasures, 7th INTERNATIONAL CONFERENCE ON FINANCIAL CRIMINOLOGY 2015 13-14 April 2015,Wadham College, Oxford, United Kingdom.

[3] BIS-CPMI, OSCO, Guidance on cyber resilience for financial market infrastructures, November 2015.

[4] Chapelle, Crama, Hubner in Peters, Practical methods for measuring and managing operational risk in the financial sector: A clinical study, 2007.

[5] Daryakin in Andriashina, Problems Of Evaluation And Management Of Operational Risks In Banks International Conference on Applied Economics, ICOAE 2015, 2-4 July 2015, Kazan, Russia.

[6] Direktiva o kapitalskih zahtevah IV (2013/36/EU), 26.6.2013.

[7] Direktiva o varnosti omrežij in informacij (2016/1148/EU), 6.7.2016.

[8] Dorogovs, Solovjova, Romanovs, New tendencies of management and control of operational risk in 9th International Strategic Management Conference, 2013.

[9] EBA, domača stran, Dostopno na: https://www.eba.europa.eu/languages/home_sl, [datum ogleda: 1. 8. 2016].

[10] EBA, Guidelines on internet payments security, december 2014.

[11] ECB, Recomendations for the security of internet payments, dostopno na: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf, 2013.

[12] ENISA NISP WG1, Risk Management Best Practice, 28.4.2014.

[13] ENISA, Inventory of Risk Management / Risk Assessment Methods, dostopno na: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods.

[14] ENISA, Inventory of Risk Management / Risk Assessment Tools, dostopno na: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools, [ogled strani: 1.8.2016].

[15] ENISA, Threat Landscape 2015.

[16] Evropska komisija, Cybersecurity Strategy for the European Union, An Open, Safe and Secure Cyberspace, 7.2.2013, dostopno na: https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

[17] Evropska komisija, European Agenda on Security, 2015, dostopno na: http://europa.eu/rapid/press-release_IP-15-4865_en.htm.

[18] Evropska komisija, Evropska agenda za varnost za obdobje 2015–2020, april 2015, dostopno na: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

[19] Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013, dostopno na: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[20] Fazlida in Said, Information Security: Risk, Governance and Implementation Setback, 7th INTERNATIONAL CONFERENCE ON FINANCIAL CRIMINOLOGY 2015 13-14 April 2015,Wadham College, Oxford, United Kingdom.

[21] FFIEC, Cybersecurity Assessment Tool - Inherent Risk Profile, June 2015.

[22] ISACA, Dostopno na: http://www.isaca.si/o_odseku.php, [datum ogleda: 1. 8. 2016].

[23] K. Lab, Kaspersky security bulletin, 2015.

[24] Kaiser, Kohne, An Introduction to Operational risk, 2006.

[25] Kazenski zakonik RS (KZ-1-UPB2, Ur.l. RS št. 50/2012, 29.6.2012).

[26] NIST, Framework for Improving Critical Infrastructure Cybersecurity, 12. 2. 2014.

[27] PWC, The Global State of Information Security Survey 2016.

[28] S. Furnell, D. Emm in M. Papadaki, The challenge of measuring cyberdependent crimes, Computer Fraud & Security October 2015.

[29] Shafer in Yildiray, Operational risk and equity prices, 2013.

[30] SI-CERT, Dosegljivo na: https://www.cert.si/si/o-centru, [ogled strani: 1.8.2016].

[31] SI-CERT, Poročilo o omrežni varnosti za leto 2015.

[32] Sklep o dokumentaciji za izdajo dovoljenj za opravljanje bančnih in finančnih storitev ter za statusna preoblikovanja, Uradni list RS, št. 72/06.

[33] Sklep o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice (Ur. l. RS, št. 73/2015).

[34] Uredba (EU) št. 468/2014 ECB z dne 16. aprila 2014 o vzpostavitvi okvira za sodelovanje znotraj EMN med ECB in pristojnimi nacionalnimi organi ter z imenovanimi nacionalnimi organi (okvirna uredba o EMN).

[35] Uredba o kapitalskih zahtevah (575/2013/EU), 26.6.2013.

[36] Uredba Sveta (EU) št. 1024/2013, 15. oktober 2013.

[37] Vlada RS, Digitalna Slovenija 2020 – Strategija razvoja informacijske družbe do leta 2020, marec 2016, dostopno na: http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/Informacijska_druzba/DSI_2020.pdf.

[38] Vlada RS, Načrt razvoja širokopasovnih omrežij naslednje generacije do leta 2020, marec 2016, dostopno na:

http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/Informacijska_druzba/NGN_2020.pdf.

[39] Vlada RS, Strategija kibernetske varnosti, februar 2016, dostopno na: http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/Informacijska_druzba/pdf/DSI2020_Strategija_Kibernetske_Varnosti.pdf.

[40] Zakon o bančništvu (Ur. l. RS, št. 25/2015).

[41] Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1, Ur.l. RS št. 98/2004, 9.9.2004).

[42] Zakon o elektronskem poslovanju na trgu (ZEPT-UPB2, Ur.l. RS št. 96/2009, 27.11.2009).

[43] Zakon o elektronskih komunikacijah (ZEKom-1, Ur.l. RS št. 109/2012, 31.12.2012).

[44] Zakon o sistemu jamstva za vloge (Uradni list RS, št. 27/16).